C TECHNOLOGIES, INC.

Knowledge Based Article
KB16008

SoloVPE Software V3.X.XXX.X Security Configuration

Abstract:	This document details the preferred Windows NTFS file security configuration for the SoloVPE software suite to properly function. These security settings play a part in the overall security plan, to be defined by each customer, to achieve their desired level of compliance with data integrity and regulatory requirements.
Applicability:	This article applies to systems with the following OS / Software combination: Windows 7 and 10 Professional (32/64-bit) SoloVPE Software Suite Version 3.X.XXX.X Cary WinUV Version 5.X.X.XXXX
Symptom:	N/A
Cause:	N/A

Detailed Info:

Different organizations and groups have been found to require different levels of security and control over their SoloVPE system. The matrix below has been prepared in order to provide guidance on the preferred security configuration for the SoloVPE software suite. 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. provides 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.

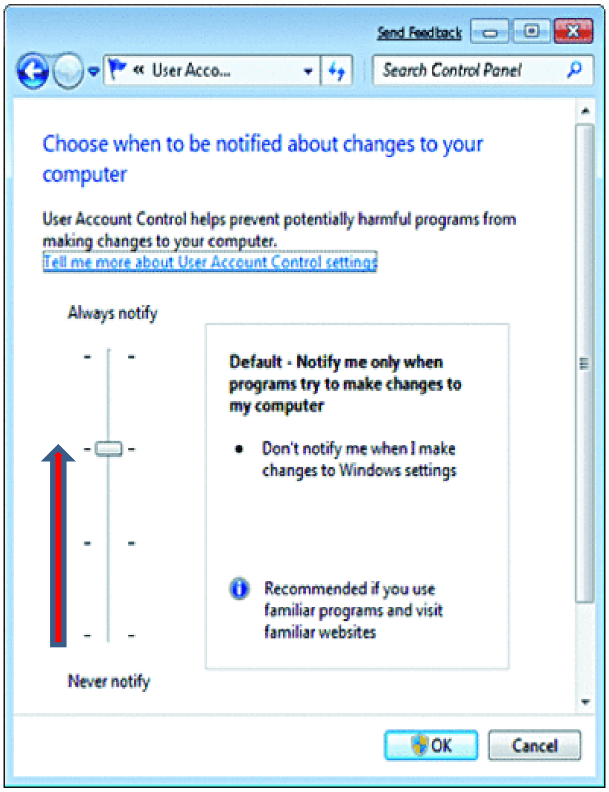
The following matrix lists and describes the standard installed folders and subfolders required by the SoloVPE software suite. The permissions noted are for all personnel who will require access to the software. Additional folders may need to be created at the discretion of the user and/or the IT group for storage and backup of data and or method files.

Windows 7 and Windows 10 have security elevation checks when users attempt to run the SecureVPE and SoloVPE Administration applications.Due to the introduction of the User Access Control (UAC) in Windows Vista and Windows 7, particular program and account permissions might demonstrate unpredictable behavior when not enabled. As a result, some of the software applications may not properly interact causing problems for the user while running the SoloVPE and SecureVPE software. Consult Microsoft's TechNet article http://technet.microsoft.com/en-us/library/2009.07.uac.aspx for detailed information on the UAC.

It is important to note that a company's active directory group policy may prevent changes to the local UAC settings from taking place. A reboot of the computer is required if the level of notification is changed. Once a computer is rebooted (and connected to a network) the active directory group policy will revert any changes to the local UAC settings.

Enable UAC (Recommended SoloVPE system setting - Default)

Turn on the UAC by moving the vertical slider to the Default position (see screenshots of examples below).



Choose when to be notified about changes to your computer

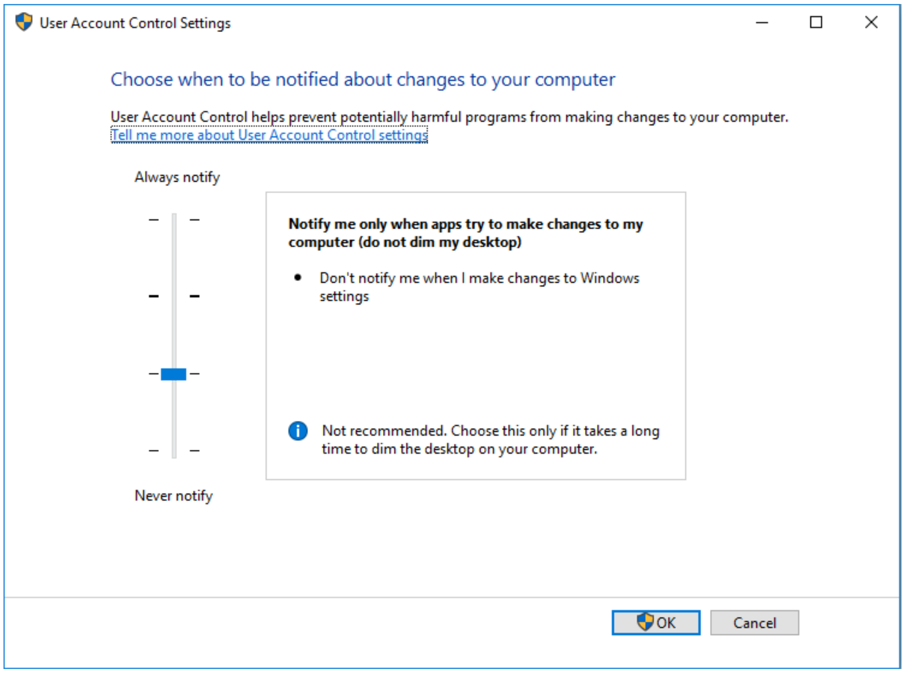
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites

Figure 1. Windows 7 UAC Configuration



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when apps try to make changes to my computer (do not dim my desktop)

- Don't notify me when I make changes to Windows settings

Not recommended. Choose this only if it takes a long time to dim the desktop on your computer.

Figure 2. Windows 10 UAC Configuration

Local Account Permissions (nondomain) As recommended by C Technologies.

Note: If the computer system was purchased from C Technologies, 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 desired administrative accounts into 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 to simulate administrative privileges. Any additional users that function at an administrator level should be added to the VPELocalAdmins group.

Standard User/Groups

Create a local group called "VPELocalUsers" and the desired accounts into 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 they should not have any elevated permissions. Add any additional standard users (non-administrator) to this group.

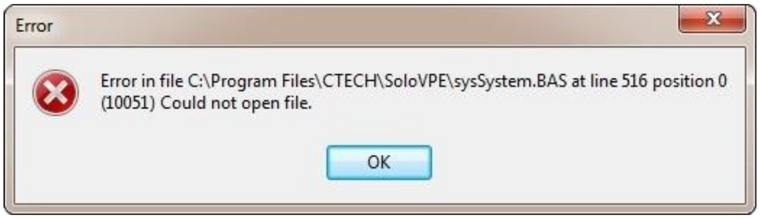
Domain-Level Permissions

Create domain-level users and add them to the appropriate security groups in the Active Directory. Grant permissions to your domain accounts following the matrix listed below.

File/Folder Security Map		
File or Folder	Description	NTFS Security
C:\Program Files (x86)\CTECH\SoloVPE\Documents	SoloVPE Documentation Folder	Read & Execute List Folder Contents Read
C:\Program Files (x86)\CTECH\SoloVPE\Hooks	SoloVPE Hooks Folder	Read & Execute List Folder Contents Read
C:\Program Files (x86)\CTECH\SoloVPE\Help	SoloVPE Help Folder	Read & Execute List Folder Contents Read
C:\Program Files (x86)\CTECH\SoloVPE\Images	SoloVPE Image Folder	List Folder Contents Read
C:\ProgramData\CTECH\SoloVPE\Solo3.db	SoloVPE System Configuration Data	Read & Execute List Folder Contents Read Write
QVCA Configuration Information (Optional)		
C:\Program Files (x86)\CTech\QVCA	Validate VPE System Folder	Read & Execute List Folder Contents Read
SecureVPE Configuration Information (Optional)		
C:\Program Files (x86)\CTECH\SecureVPE\	SecureVPE Interface Application	Read & Execute List Folder Contents Read
C:\ProgramData\CTECH\SecureVPE\	SecureVPE Configuration Data	Read & Execute List Folder Contents Read Write

Table 1: File / Folder Security Map

Common Error:



Error in file C:\Program Files\CTECH\SoloVPE\sysSystem.BAS at line 516 position 0
(10051) Could not open file.

Figure 3: 10051 Error could not open file / 10021 Error could not open file

This error message (or similar) is likely caused by improper permission settings on the following folder:
C:\ProgramData\CTech\SoloVPE

Document Info: KB16008

Revision History			
Rev	**Date**	**Changes**	**Initials**
00	2016-10-12	Initial revision	JF
01	2017-01-17	Updated to account for a software version release	JF
02	2018-04-13	Updated to account for a software version release	JF
03	2019-12-18	Accounted for Windows 10 and added in conflicts with Active Directory group policy	JM

Prepared By:

C Technologies, Inc.
685 US Route 202 Bridgewater, NJ 08807
☎ (908) 707-1009
✉ support@ctechnologiesinc.com