

VPE Software: FlowVPE Software Security Configuration

Abstract: This document details the preferred Windows security configuration for the FlowVPE software, specifically the permissions for the files and folders associated with the FlowVPE software suite and the GLP administration application. These security settings are a part of an overall security plan to be defined by each customer to achieve their desired level of GxP compliance.

Applicability: This article applies to the FlowVPE software running in the Agilent Cary WinUV (Version 5.0 and higher) environment on a computer running the Windows 7 or 10 Professional (32/64-bit) operating system with an NTFS file permission on the system. Applies to system running FlowVPE software suite V1.X.XXX.

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 FlowVPE System. To provide guidance on the preferred security configuration on the FlowVPE software, the matrix below has been prepared. It is up to the customer's Information Technology (IT) 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.*

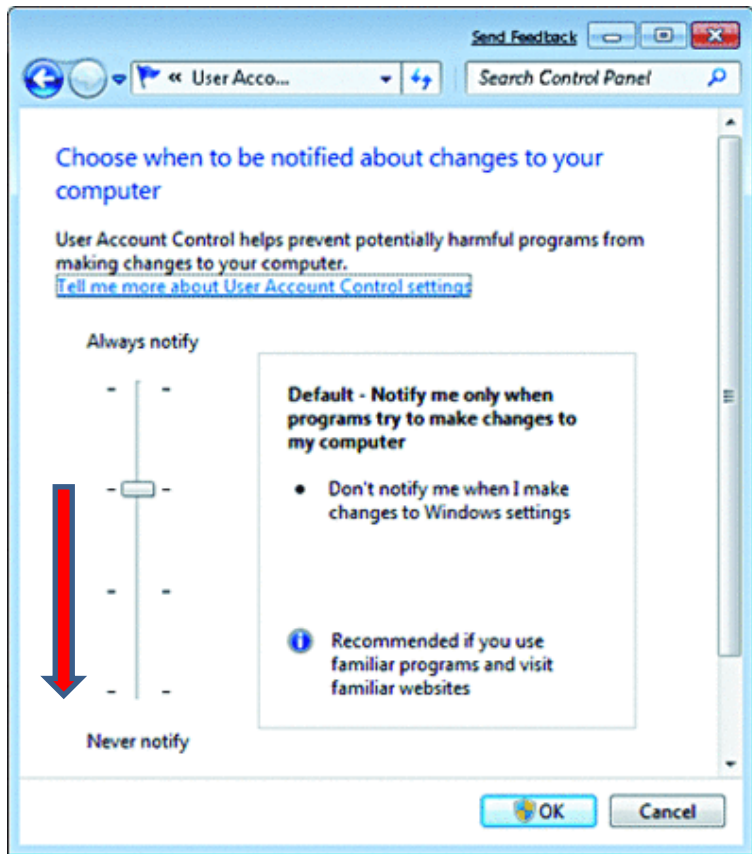
The following matrix lists and describes the standard installed folders and subfolders required by the FlowVPE software. The permissions noted are for non-administrative personnel. For each folder and/or file, the preferred security permissions are listed that provide the appropriate level of protection to operate the FlowVPE software. Administrative privileges will be required to perform updates on the FlowVPE System to 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.

Because of 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 and cause problems for the user while running the FlowVPE and GLP administration software. Consult Microsoft's TechNet article <http://technet.microsoft.com/en-us/library/2009.07.uac.aspx> for detailed information on the UAC.

Enable UAC (Default SoloVPE System setting)

Turn on the UAC by moving the "slider" to the Never Notify position (see screenshot below). Windows 7 will not have security elevation checks when users attempt to run the FlowVPE software.



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

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 group by following the matrix specified below. These are the minimum NTFS permissions that are to be granted to the 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 user called "VPELocalUser" and a group called "VPELocalUsers" and add VPELocalUser user account to this group. Assign permissions to the VPELocalUsers group by following the matrix specified below. Keep in mind that these are minimum permissions for a standard user to run the FlowVPE software and should not have any elevated permissions! Add any additional standard users (nonadministrator) to this group.

Domain-Level Permissions

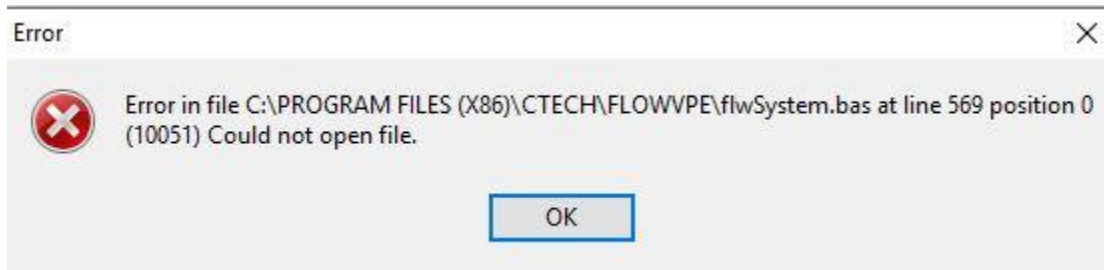
Create domain-level users and add them to the appropriate security groups in the active directory. Grant permissions to your domain accounts following the matrix listed below. Once the active directory is involved, IT is responsible for all the permissions of the groups and/or users.

File/Folder Security Map		
File/Folder	Description	NTFS Security
C:\Program Files (x86)\CTECH\FlowVPE (For 32-bit computers, C:\Program Files\CTECH\FlowVPE)	FlowVPE Files Folder	Read & Execute List Folder Contents: Read Write
C:\ProgramData\CTECH\FlowVPE	FlowVPE Data Folder	Read & Execute List Folder Contents: Read Write Delete
C:\Program Files (x86)\Agilent\CaryWinUV	Cary WinUV Files Folder	Read & Execute List Folder Contents: Read Write
C:\ProgramData\Agilent\CaryWinUV	Cary WinUV Data Folder	Read & Execute List Folder Contents: Read Write Delete
Save Path Location		
C:\Users\Public\Documents\cTechnologies\FlowVPE\RunData	FlowVPE Database Files	Read & Execute List Folder Contents: Read Write

Troubleshooting Specific Permissions

The error message below is caused by improper permission settings in the following folder:
C:\ProgramFiles (x86)\CTech\FlowVPE and C:\ProgramData\CTech\FlowVPE

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



Document Info:

Revision History			
Rev	Date	Changes	Initials
00	2019-06-28	Initial Release	BG

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