Preventing the modification of .BVP files within the ADL Shell / Cary WinUV Environment

Abstract: This document outlines the potential risk for data modification outside of the SoloVPE Software and provides, in detail, suggested Windows NTFS security configurations for a secured network data storage location. These configurations will prevent unauthorized access to SoloVPE data and prevent data storage to unauthorized locations. C Technologies, Inc. recommends that all data is saved to a secured network location.

Applicability: This article applies to SoloVPE Software V3.X.XXX running in the Agilent Cary WinUV (Version 5) environment on a **Windows 7 Professional (32/64-bit)** or **Windows 10 Professional (32/64-bit)** operating system with an NTFS file system on the system hard disk.

Symptom: Not Applicable

Cause: Should a user open an ADL Shell window (Independent of the SoloVPE Software or unconnected to the current SoloVPE Software window), it is possible to overwrite and or modify .BVP files.

Definitions:
ADL Shell: Scripting language designed to manipulate the Cary WinUV environment
.BVP/batch file: The file extension SoloVPE software uses for data
NTFS: NT File System permissions are used to manage access to data stored
SoloVPE Software: A software module used to run SoloVPE system
SecureVPE: An add-on module that configures the User/Group permissions for SoloVPE and QuickVCA software modules
Cary WinUV Software: The software environment that interfaces directly with the Cary 60
Cary 60: A model of spectrophotometer used with the SoloVPE instrument
Users: End users of SoloVPE, people who use the SoloVPE to analyze samples

Detailed Information:

The following steps outline how to organize permissions to a network folder where users can save all data generated by the SoloVPE Software, but not modify or delete the data. The prevention of unauthorized modification of data is key to having a compliant system. For companies that wish to prevent users from viewing any data after it is saved we recommend removing the permission “List folder contents”. This prevents users from seeing any files should they open file explorer.

Note: Inherited permissions must be disabled to fully secure the files.

For users wishing to save locally instead of on a network drive, the VPE System Service needs to be installed and running so that the user that is creating the data is not the owner of the data. Windows NTFS permissions when mixed with file ownership cause conflict and cause users to have more rights than assigned in Security. To help overcome this issue C Technologies Inc. has added the VPE System Service feature to SoloVPE Software v3.1.

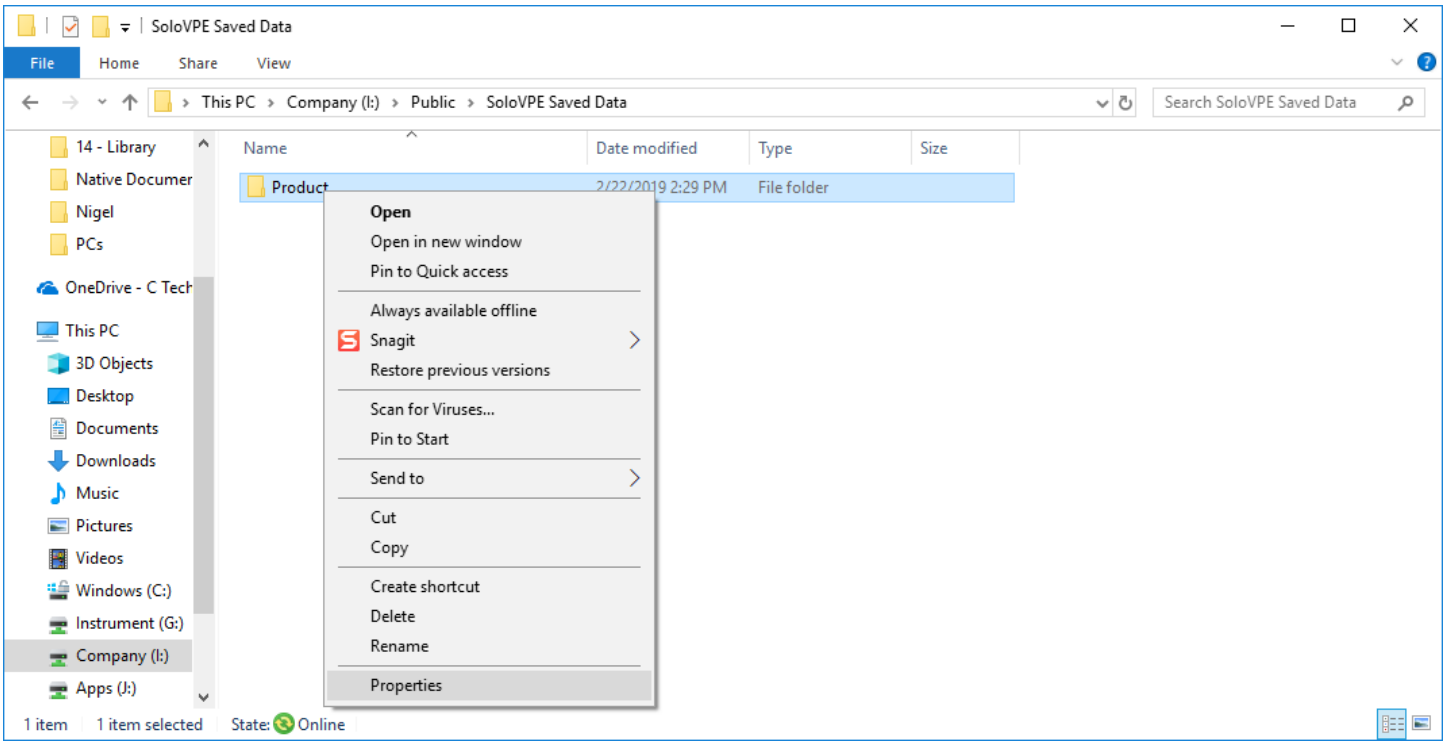
A set of permissions exist that blocks users from viewing files in a folder where users should be saving all data to, but still being allowed to write to it. (Essentially, a folder that they can see exists, but the contents are invisible and untouchable). This allows data to be securely stored and accessed for review (by authorized users) without fear of manipulation.

Users must have their permissions explicitly set this way so that any unauthorized editing, modification, or deletion is prevented.

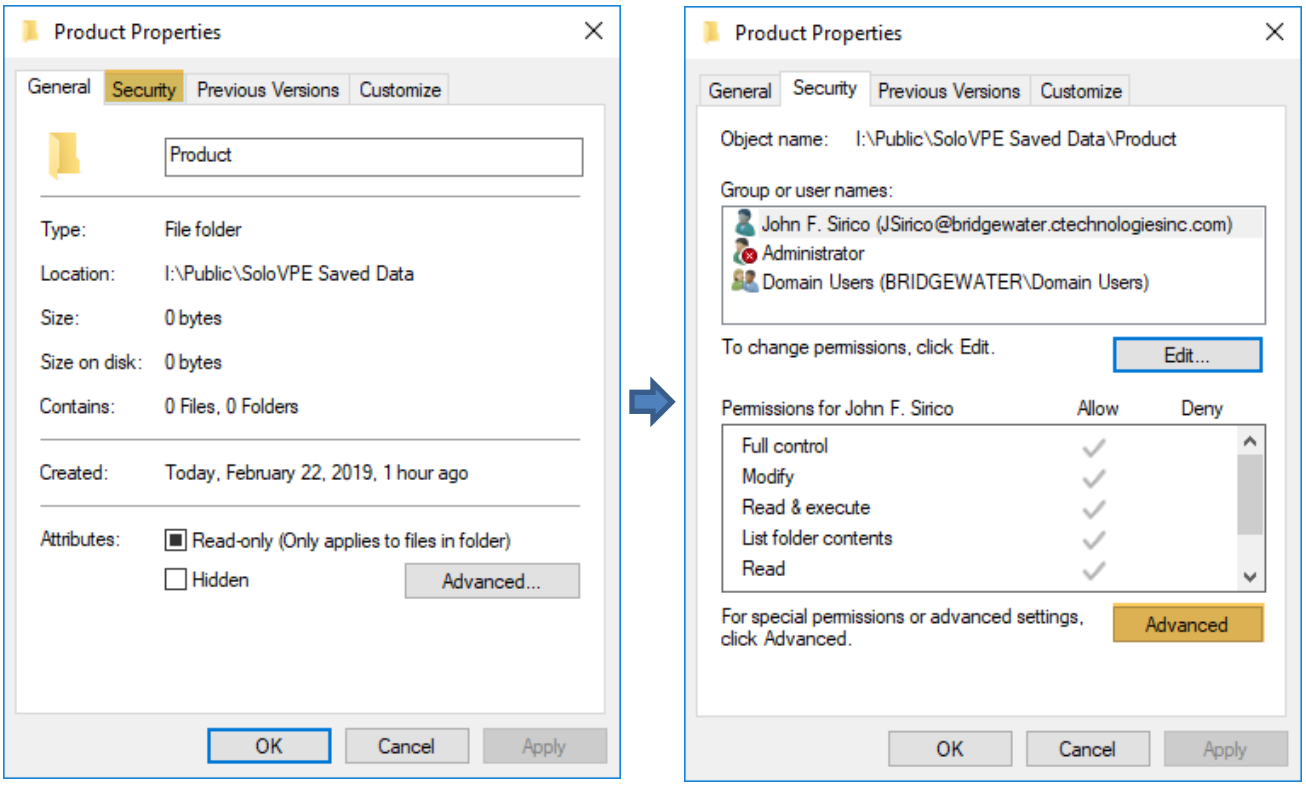
Windows 10:

1. To determine who has access and to correct the issue, navigate to the Default Save Path location and right click on the folder.

2. Select Properties.

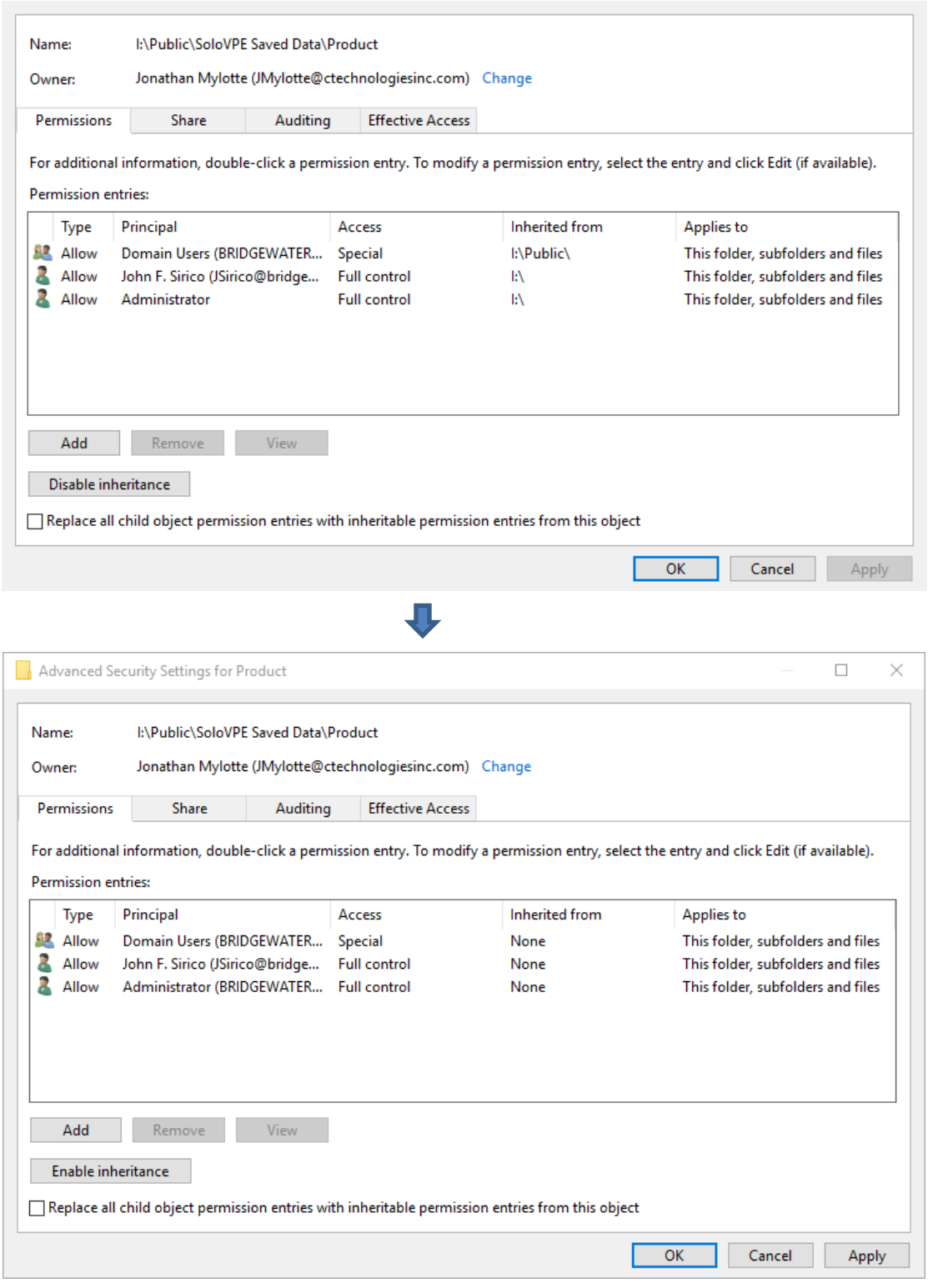


3. Select the Security tab and click Advanced



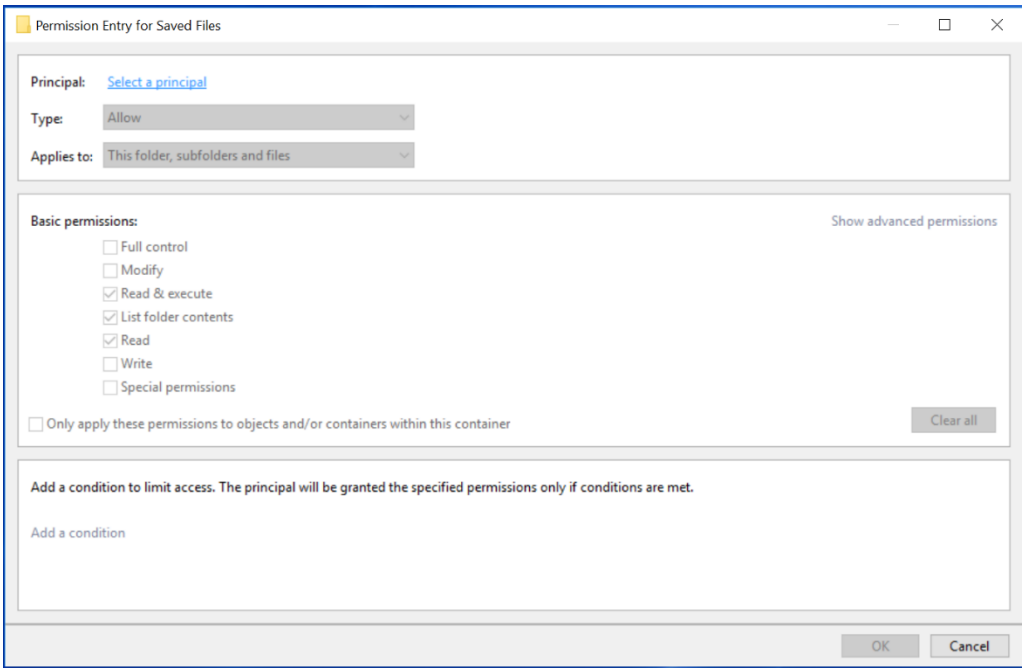
4. Ensure that “Replace all child object permission entities with inheritable permission entities from this object” is checked off.

5. Disable Inheritance for all users listed.

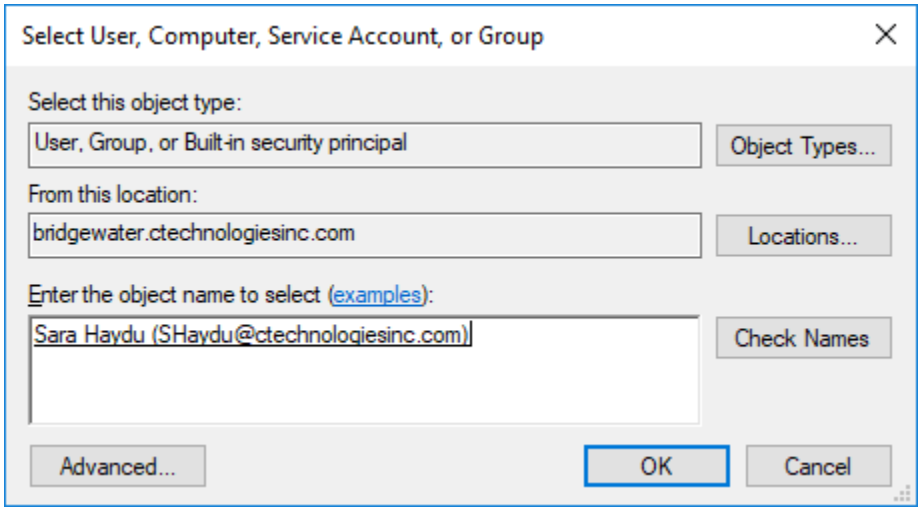


6. To add a user to the list, click “Add”.

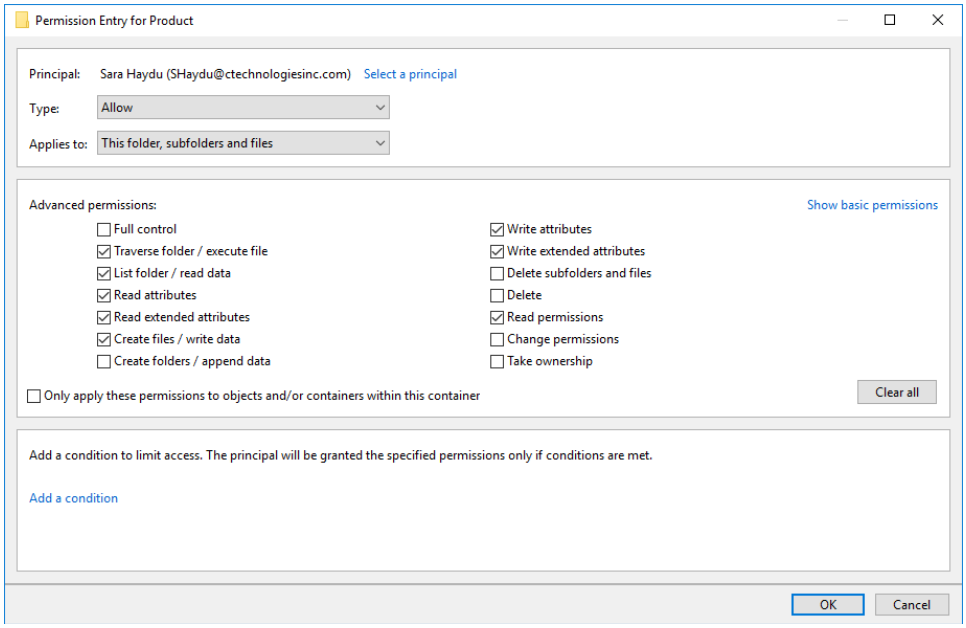
7. Click on “Select a principal”.



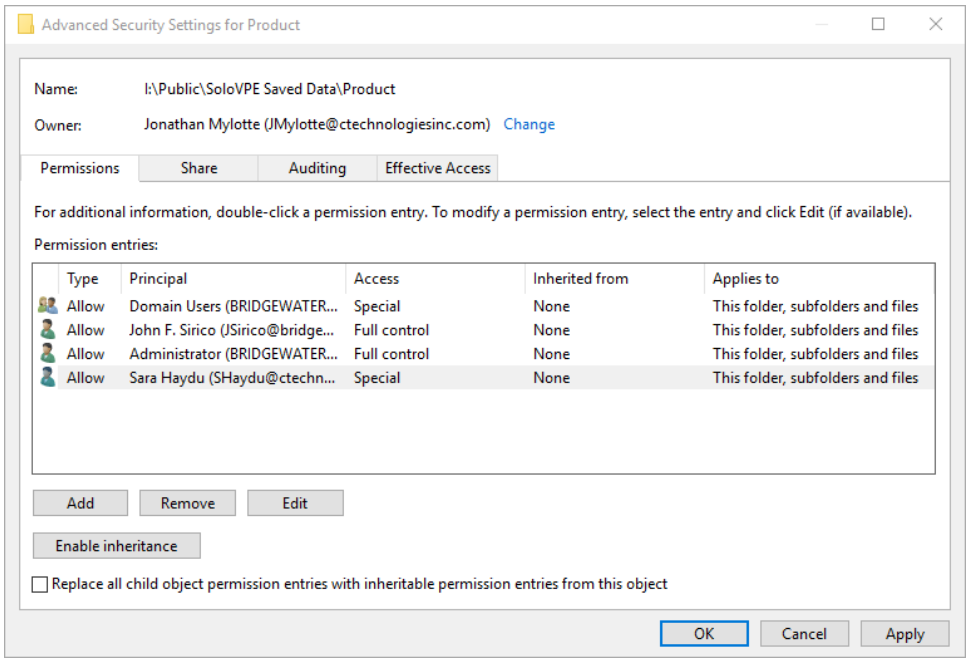
8. In the pop-up, type the users name and click “Check Names” to pull up their active directory user account. Then click “OK”.



9. Click on “Show advanced permissions”.
10. Set the permissions for each user according to the following figure. Then click “OK”.



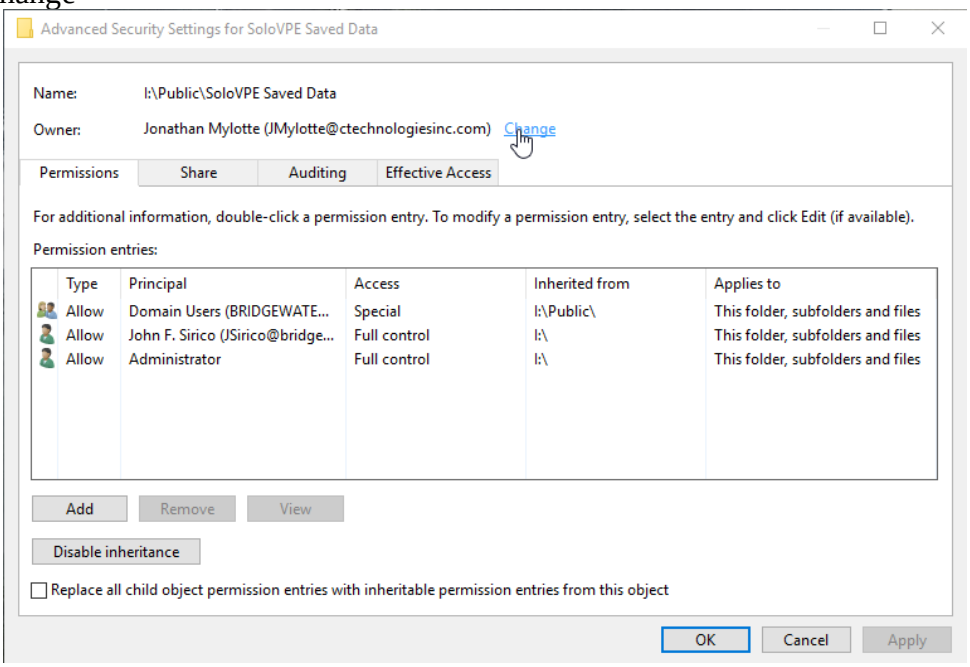
11. Once all users have been accounted for, click “Apply” and “OK”.



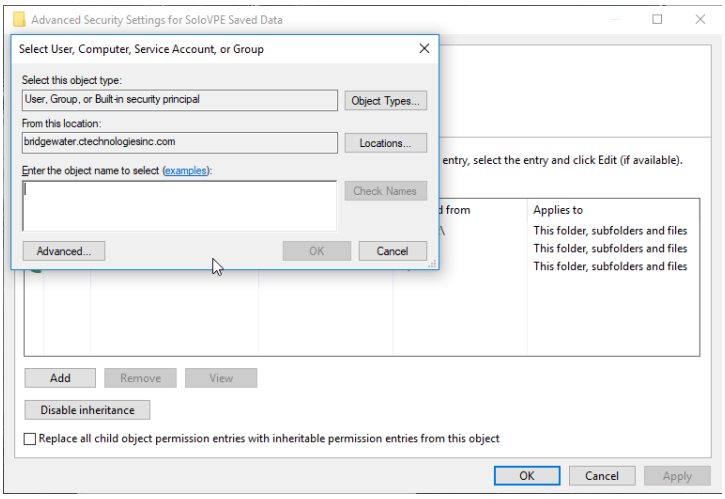
Note:
Folder ownership is recommended to be a network administrator, especially a user or group that is not involved in the generation or review of data in the laboratory.

Folder ownership is modified as follows:

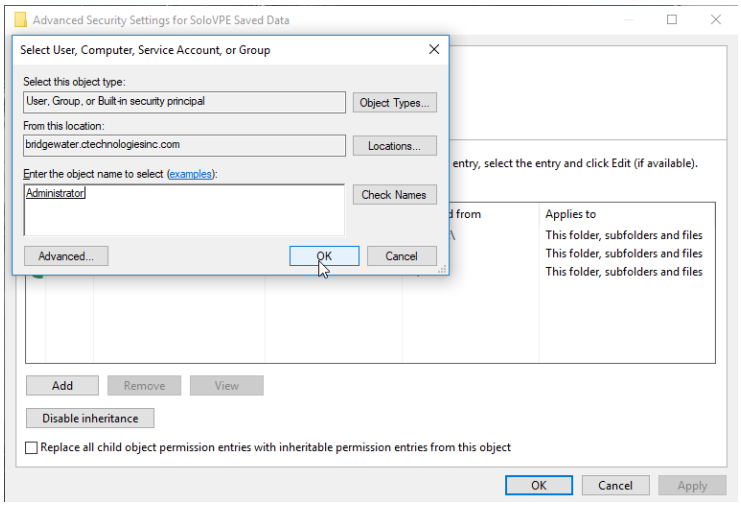
1. Click on Change



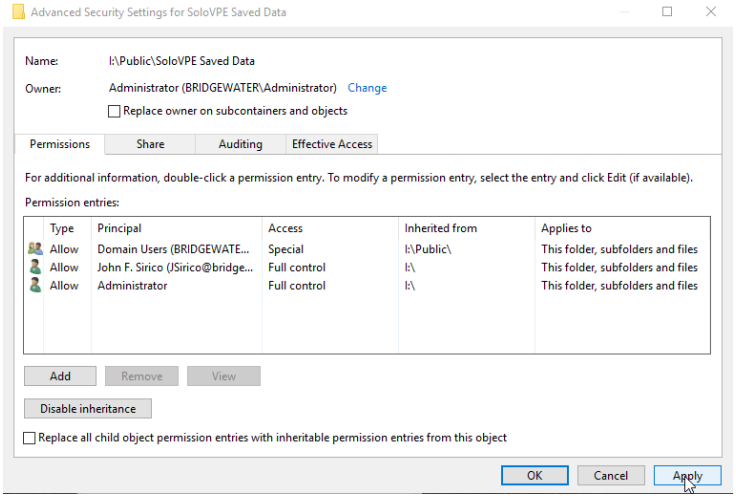
2. Type in the name of the Administrator or the Administrator group.



3. Click OK once the user or group has been identified

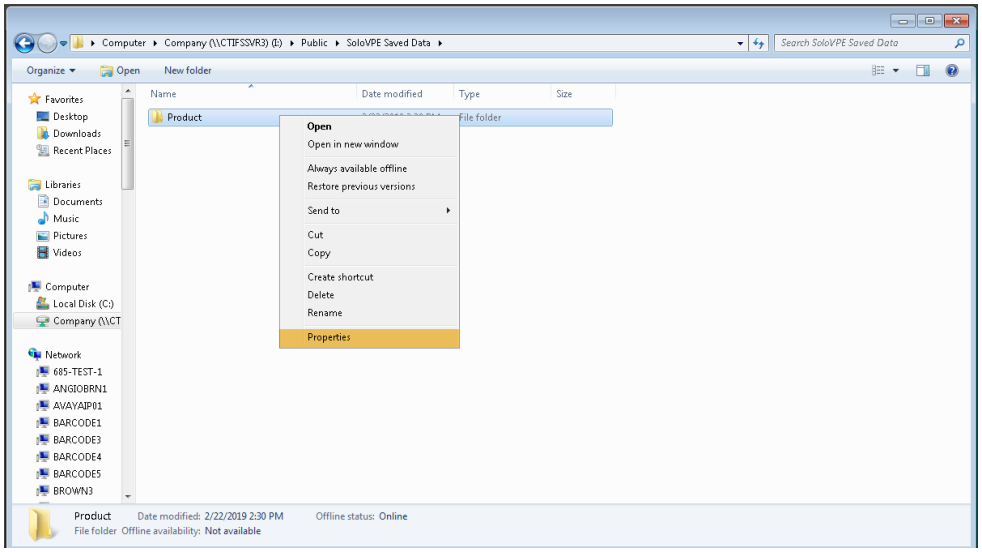


4. Click Apply once done

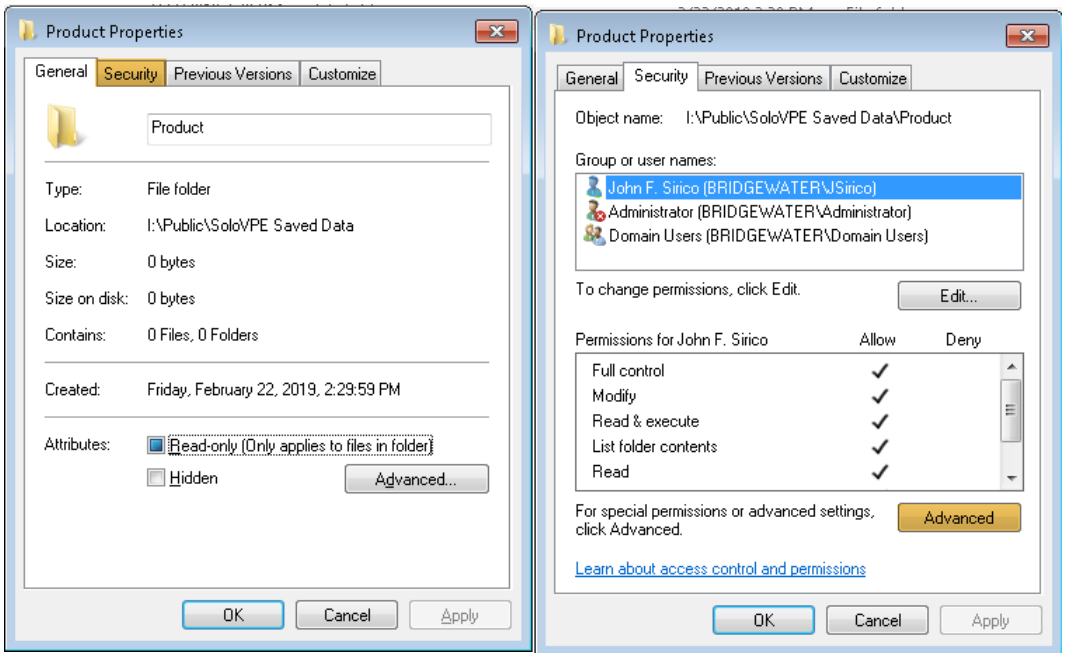


Windows 7:

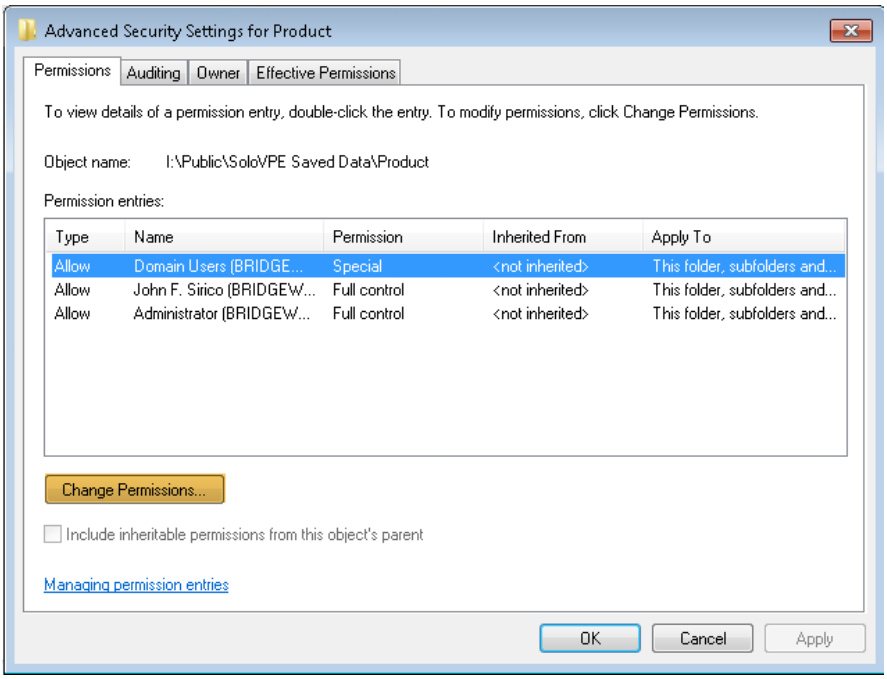
1. To determine who has access and to correct the issue, navigate to the Default Save Path location and right click on the folder.
2. Select Properties.



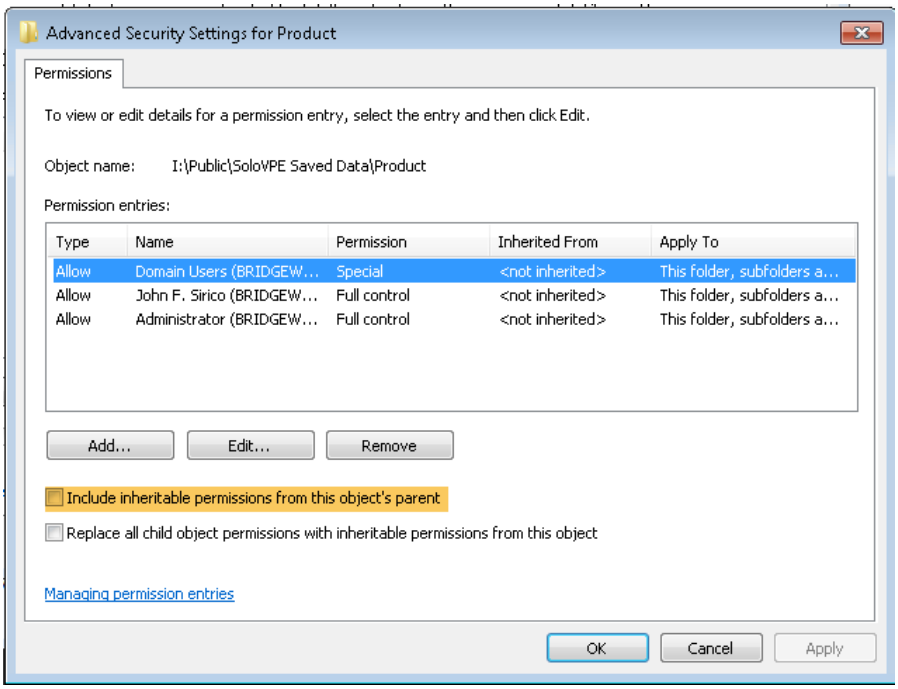
3. Select the Security tab and click “Advanced”.



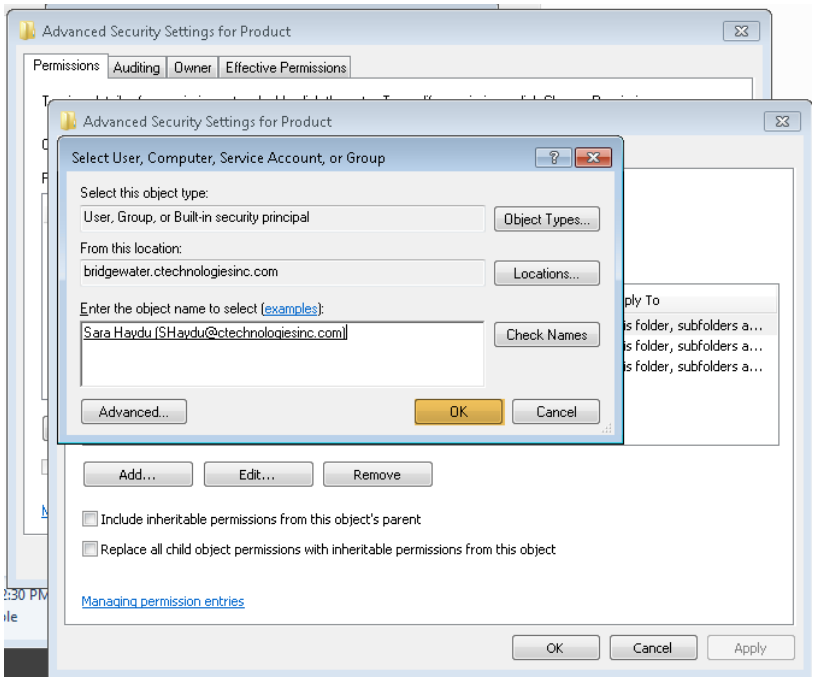
4. Click on “Change Permissions”.



5. Uncheck “Include inheritable permissions from this object’s parent”.

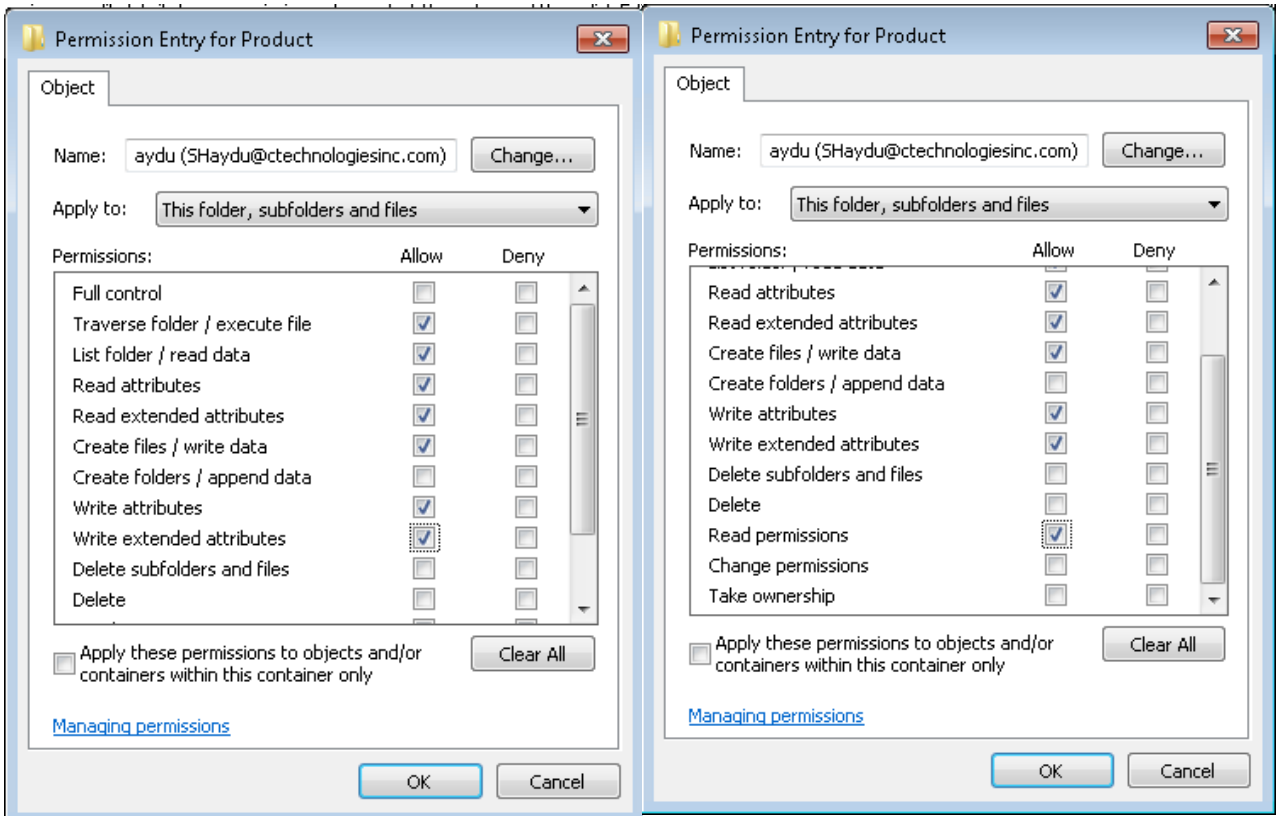


6. Click “Add” to modify those users already listed in the Advanced Security Settings for the default save path location. Once you locate the user or group to add, click “OK”.

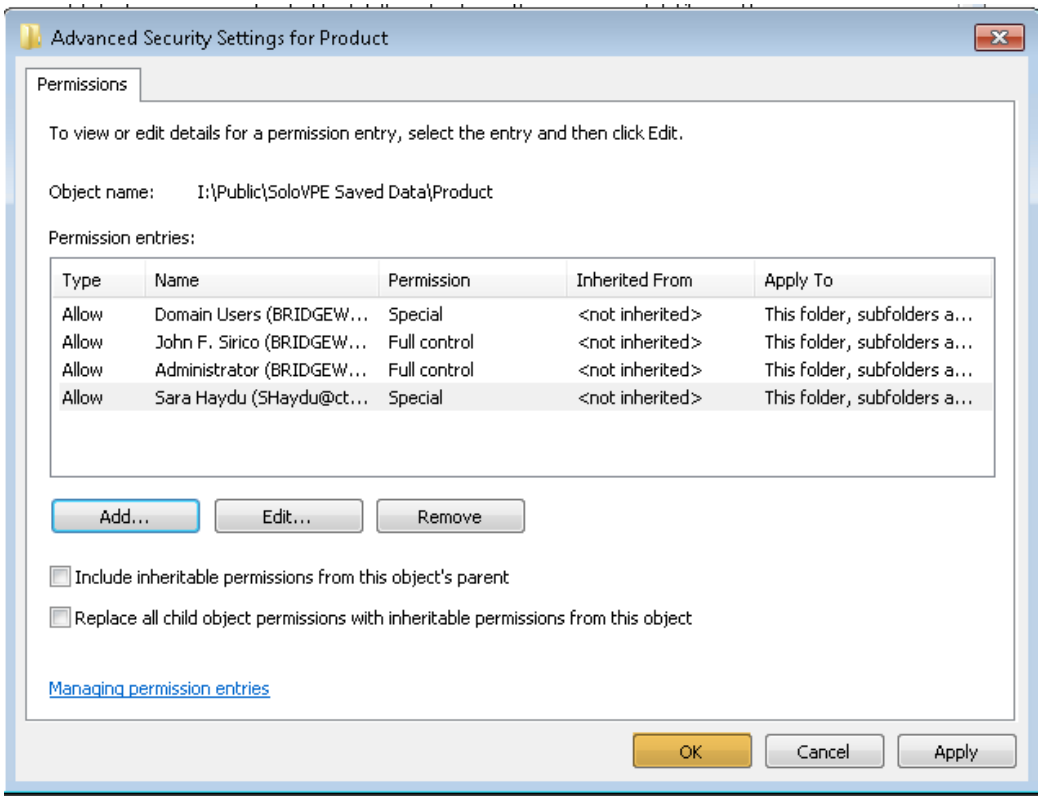


7. Double click on each user to modify their permissions.

8. In the Permission Entry for the default save path location's Pop-up, ensure that only the following boxes are checked. Then click OK.

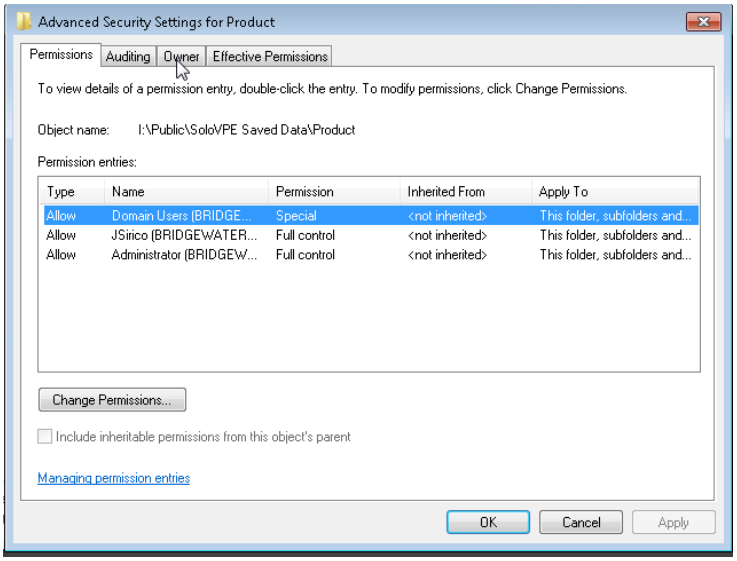


9. Click Apply and OK

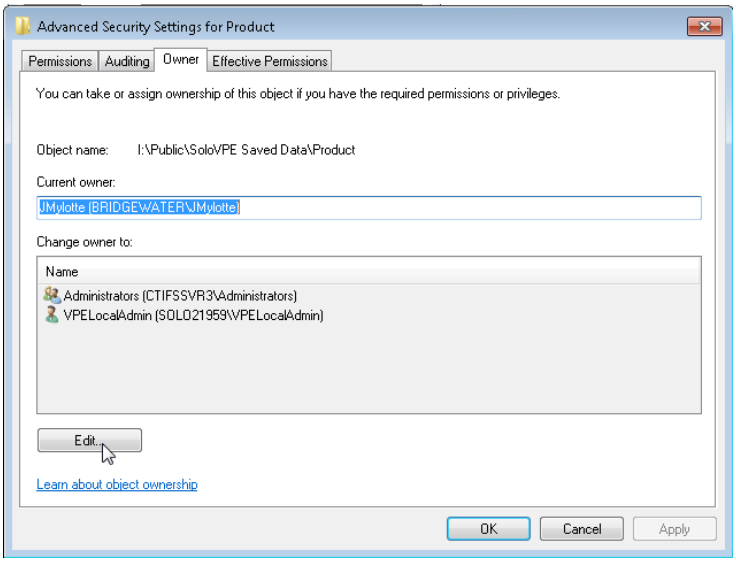


Folder ownership is modified as follows:

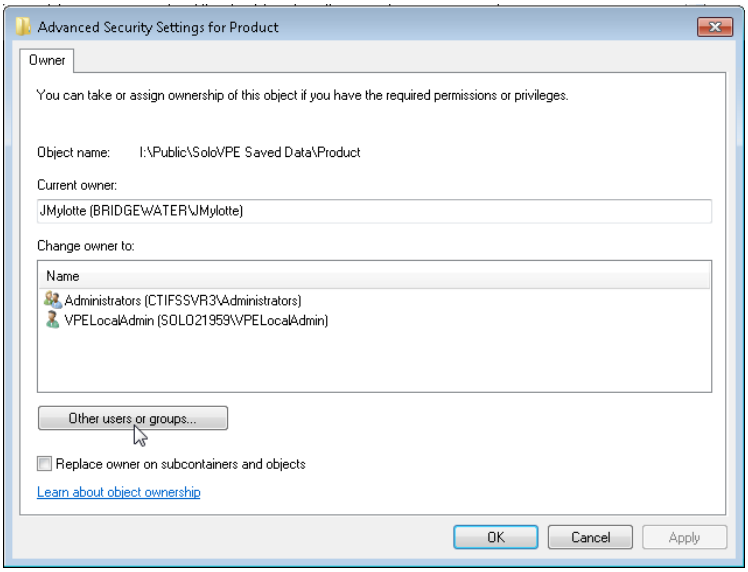
1. Click on Owner tab



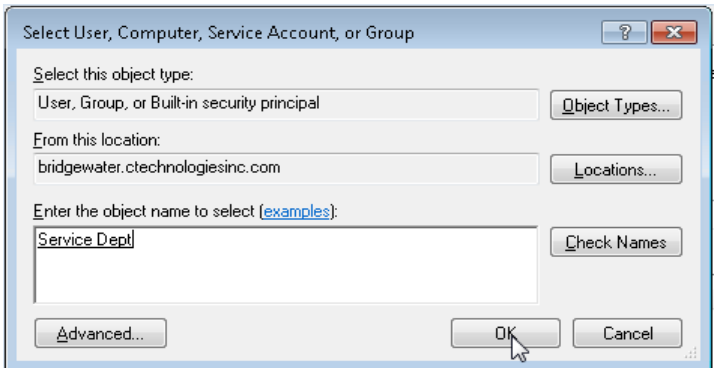
2. Click Edit to modify the folder owner



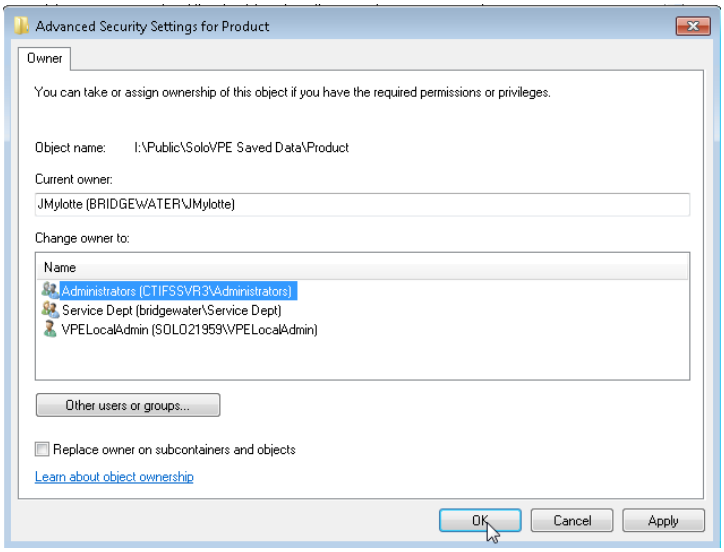
3. In the Advanced Security Settings for Product pop-up if the user or group you want to own the folder is not listed click on Other users or groups. If the user or group is listed skip to step 5.



4. If you click on Other users or groups then type their name in the pop-up, click Check Names and click ok. Skip to step 5 if you chose from the available list in step 3.



5. Select the name from the list and click OK



Document Info:

Revision History			
Rev	**Date**	**Changes**	**Initials**
00	2019-04-22	Initial Release	JM

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