SPRAYTEC 2000
SECURING FILES FROM DELETION

With a 21CFR11 compliant computer system, one of first concerns to address is the potential for the loss of data; either accidently, or by intention. Utilizing the built-in security tools of Microsoft® Windows®, an IT professional can change user access to specific files and/or folders by removing certain file/folder permissions.

Before configuring Windows file/folder permissions

Before configuring the Windows file and folder permissions, there are several actions the customer must take, or at least consider. Connecting the PC to a company network is the preferred option – this allows for remote IT support, virus protection, user authentication and most importantly data archiving.

A networked PC

The PC should have been configured by the local IT department to include the following:

1. Connection to the company domain to allow secure user authentication.
2. Anti-virus software.
3. Any remote administration software.
4. An instrument user group should be created locally, or within the AD.
5. Any company group policies (GPO) should be started.
6. A reliability check of the LAN connection.

Non-networked PC

1. A local Administrator account and password must be set-up.
2. A local user group should be set-up (optional but recommended).
3. Local users should be created with passwords, limiting users to be 'Standard Users' within Windows.

Note:
A backup policy for copying data from the instrument PC to a network, or saving data directly to a specific network location, must be considered. For non-networked computers, backing up to an external hard-disk, CD/DVD writable media, or tape/DAT drive should be considered.

Installing the Spraytec Application Software

The Spraytec application software should follow a standard installation plan. *Figure 1* illustrates the installation process starting with the application software and ending with the configuration of the folder security. Installing the software and configuring the Windows security requires a Widows Administrator account.

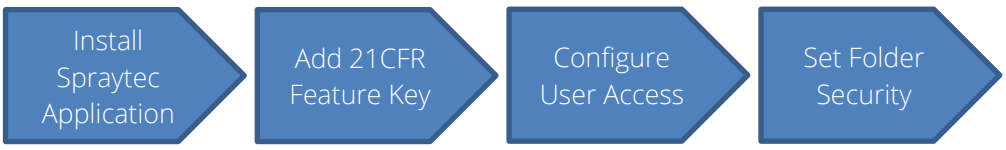

Figure 1. Typical installation process required for validated systems.

Protecting critical folders

When the Spraytec application is installed, a directory structure is created to give control over the data files created during a measurement. For the Spraytec software to be operated in a way that is 21 CFR Part 11 compliant, the operating system must be set up to ensure that Spraytec data files cannot be deleted, either from within the Spraytec application or using other applications such as Windows File Explorer™.

The runtime files and folders require no additional protection, as deletion or other manipulation would typically result in the application failing to start. However, output files like measurement data, SOPs, and Audit History could be deleted without initially being noticed, potentially causing a compliance issue. To avoid this risk, these files must be protected from deletion by setting the Windows-based security at the folder level.

Table 1 below identifies the important folders that should be secured for most typical installations, where protection is a 'Must' - Other less frequently utilized folders are marked as 'If Used'.

Table 1. Folders where security should be applied.

Folder	Protection Required
C:\ProgramData\Malvern Instruments\Spraytec\Security	Must
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Acrobat Results	Must
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Audit Trails	Must
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Measurement Data	Must
C:\Users\Public\Documents\Malvern Instruments\Spraytec\SOP	Must
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Backup	If used
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Export Data	If used
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Export Templates	If Used
C:\Users\Public\Documents\Malvern Instruments\Spraytec\Import Templates	If Used

Changing folder security

For the next part of this document, it is assumed that you have the required administrator rights for the system; allowing you to install, or update software and configure windows security permissions.

The following example shows how to change the folder permissions on the Audit Trail folder on a non-networked PC. Malvern Panalytical strongly advise that customers seek the help of IT professionals when implementing security changes.

Note:
For the following example, we have previously created a user group, through the Computer Management console, called 'Spraytec Operators'. This user group will later be added into the folder permissions of the Audit Trails folder to prevent users from deleting records. This process can be applied to any output folder requiring limited user access.
We have not removed default groups such as 'Everyone' or 'Users' - these can be deleted or used as an alternative to dedicated user group/s. However, when using these groups, we strongly advise that explicit 'Denies' are not used, unless you fully understand the Microsoft file/folder security permissions.

1. Navigate to one of the folders that needs to be secured - in this case we have selected the folder where the Spraytec audit trail files are stored. Right-click on the folder and through the context menu open the folder **Properties**.
2. In **Audit Trails Properties**, select the **Security** tab and click the **Advanced** button to open the **Advanced Security Settings**.

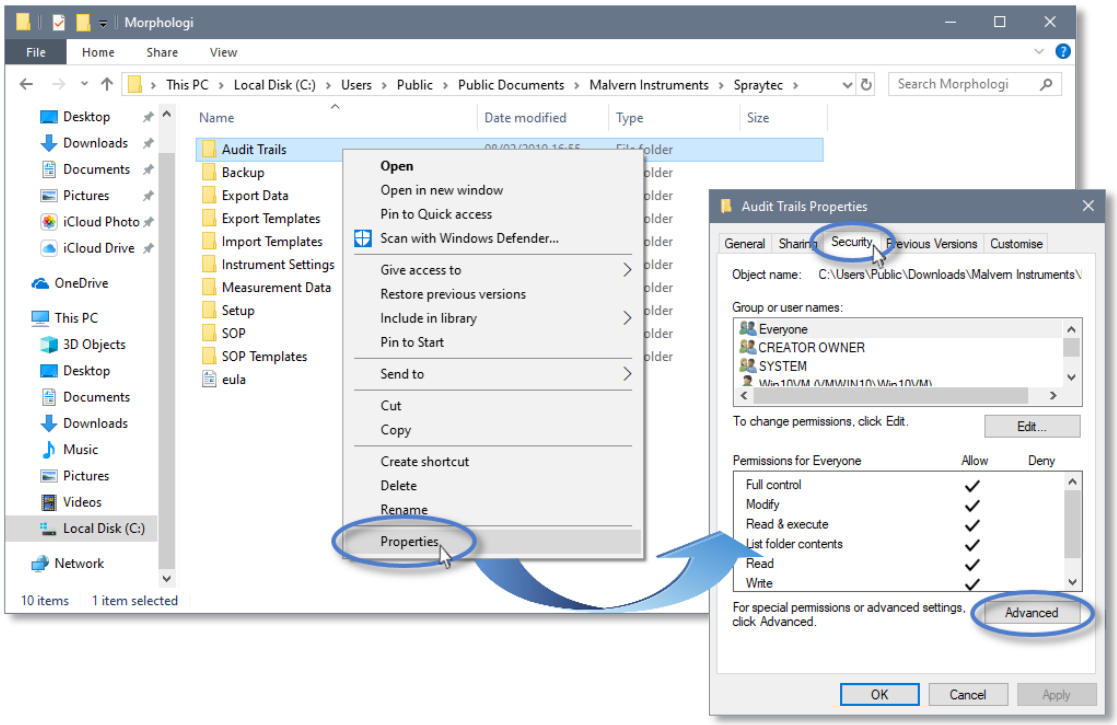

Figure 2. Find advanced security settings

3. Click the **Disable inheritance** button in the **Advanced Security Settings.** If this button is not available, you will need to click the **Change permissions** button first.

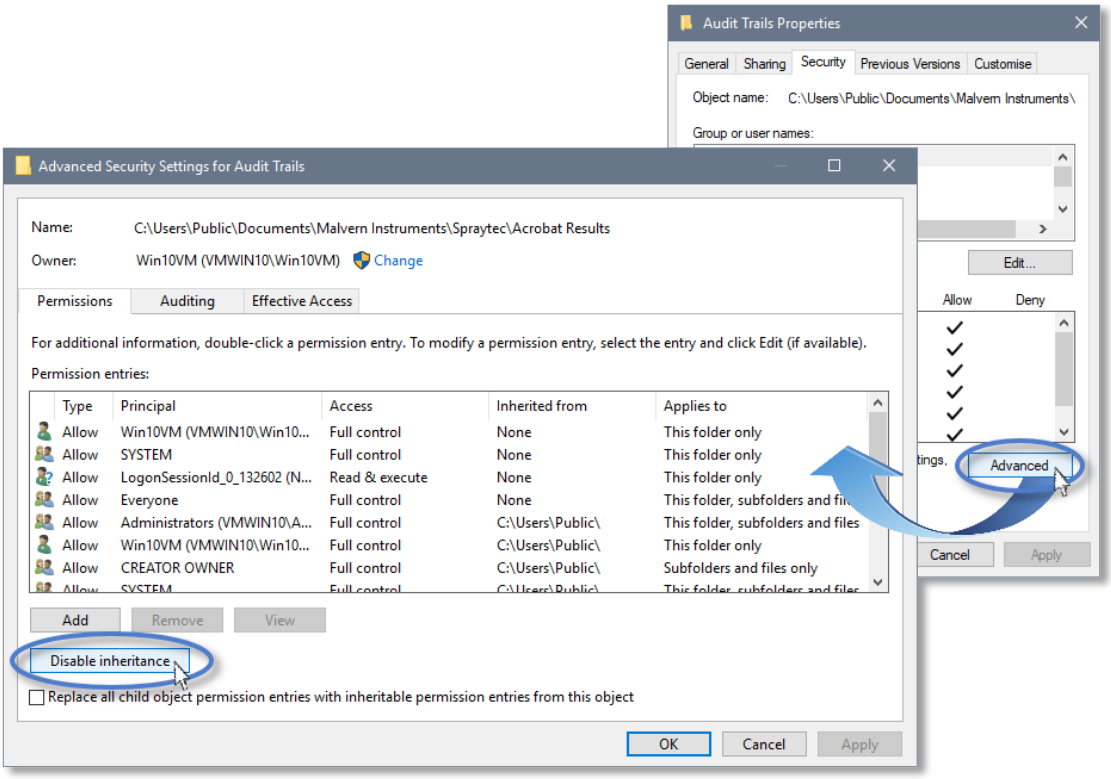

Figure 3. Disable inheritance

4. In **Block Inheritance**, click **Convert inherited permissions into explicit permissions on this object** – this removes the permission inheritance from the parent folder, whilst keeping the any current users and groups settings.

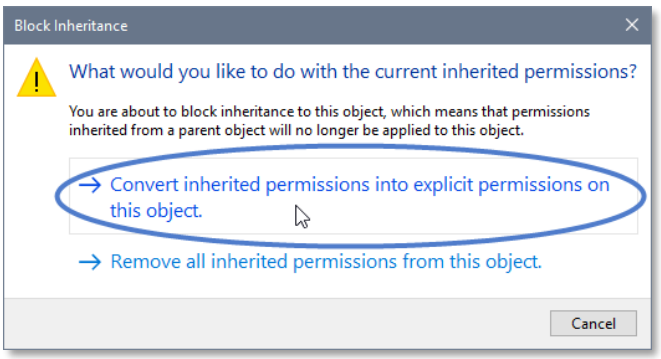

Figure 4. Block Inheritance

5. After returning to the **Advanced Security Settings** window, select the **Spraytec Operators** group and then the **Edit** button.
6. In the **Permissions Entry** window, click **Show advanced permissions** to reveal the full permissions list.

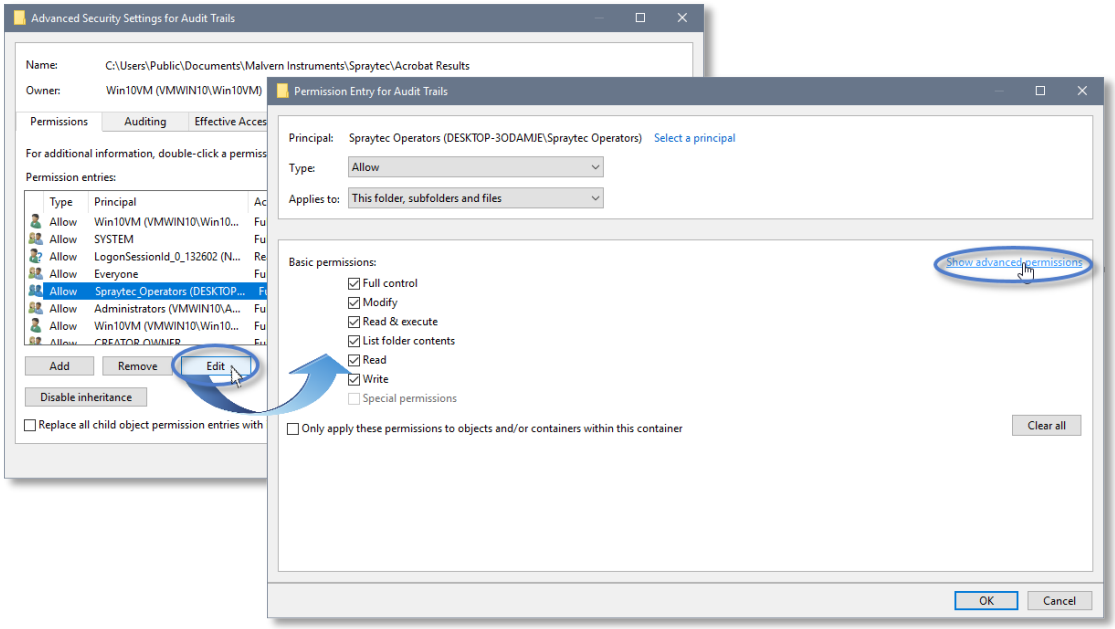

Figure 5. Full permissions list

7. Deselect the checkboxes of **Delete subfolder and files**, **Delete**, **Change permissions**, **Take ownership** and finish by clicking the **OK** button to return to the previous window.

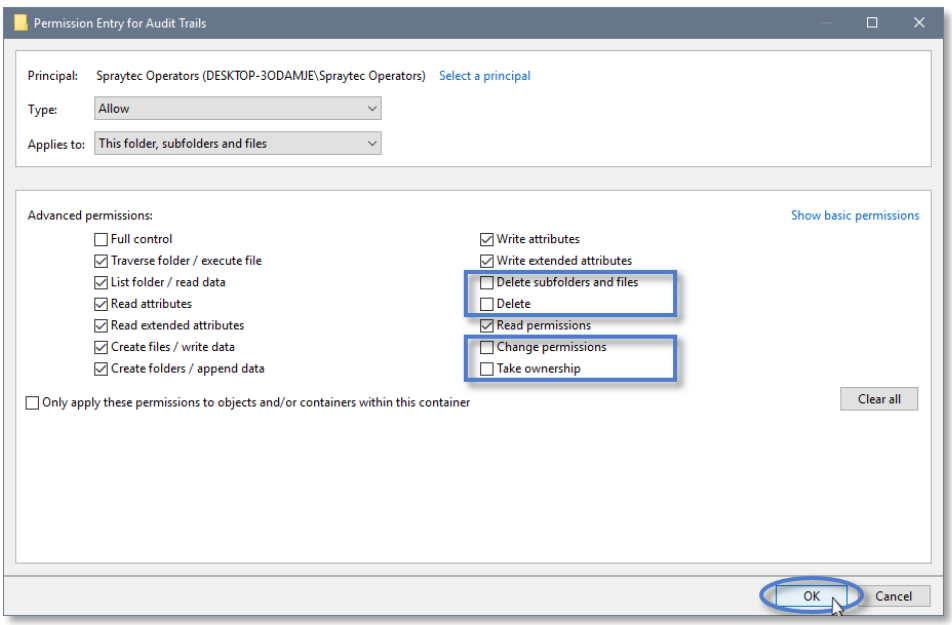

Figure 6. Permissions checkboxes to deselect

8. Click **Replace all child permission entries with inheritable permission entries from the object** and click the **Apply** button.
9. Click the **Yes** button when prompted to replace the permissions and the **OK** button when you return to the previous window.

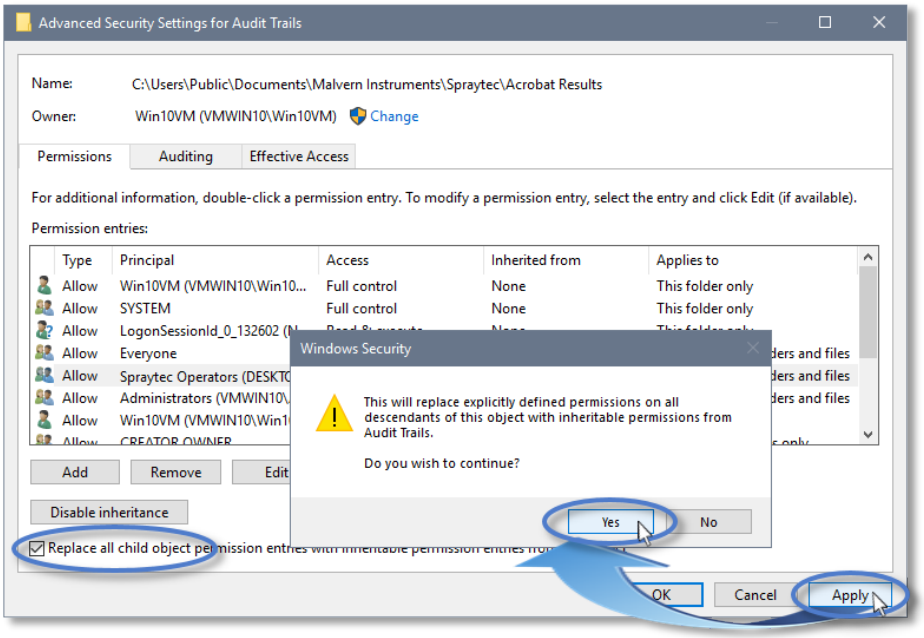

Figure 7. Confirm permission replacements

10. Click the **OK** button when you return to original folder properties window to confirm your security changes.

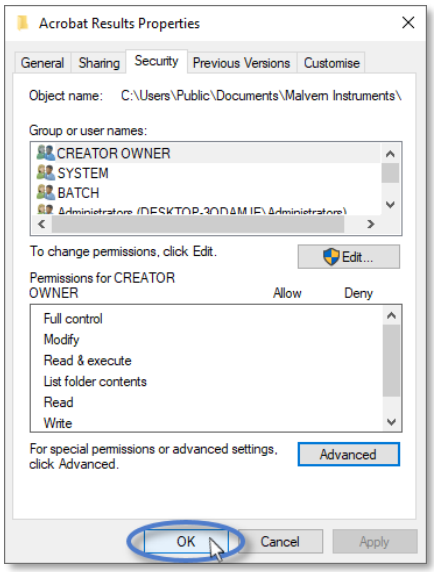

Figure 8. Confirm changes to permissions

Malvern Panalytical
a spectris company

MALVERN PANALYTICAL

Malvern Panalytical Ltd.
Grovewood Road, Malvern,
Worcestershire, WR14 1XZ,
United Kingdom

Tel: +44 1684 892456
Fax: +44 1684 892789

Malvern Panalytical B.V.
Lelyweg 1, 7602 EA Almelo,
The Netherlands

Tel: +31 546 534 444
Fax: +31 546 534 598

info@malvernpanalytical.com
www.malvernpanalytical.com