

Installation of Version 3.00 software for Mastersizer Legacy Systems.

22nd January 2003

Who should read this document?

This document has been produced as a Guide to user Companies' Systems Administrators and IT Personnel concerned with configuring their company's Legacy Mastersizer systems to enable them to maximise their compliance with the requirements of 21 CFR part 11.

It should be read in conjunction with the QSpec software update notification to be found on the Version 3.00 CD Rom Part No.PSS0008-01, together with the References listed at the end of this note.

1) Before installation

- a) Make sure that you have purchased a licence code for this version of software before installing it.
- b) If you do not have a licence code, you should contact Malvern Instruments to purchase one. You will need to know the serial number of the specific Mastersizer instrument that you propose to use with the version 3.00 software.
- c) Check that your internal protocols relating to upgrading software have been observed.
Such protocols will probably include reviewing the changes that have been made to the software since your current version was installed.
- d) To do this, insert the CD Rom into the drive of your computer and, using Explorer, open the QSpec Update Notification.pdfs in the *Information* directory on the CD. Separate Notifications have been included for each of the Versions of software introduced after V2.16.
- e) You will also find Legacy Systems ER & ES Advice.pdf which should be printed out and read in conjunction with this document.
- f) Make sure that your operating system is Windows NT 4.0 SP 6a, Windows 2000 SP2 or Windows XP SP1 or later.
Section 7.2 of the QSpec Software Update Notification has further details of system requirements. Print this document for ease of reference during the installation procedure.

2) Setting up Windows NT Security.

This **must** be the ultimate responsibility of your IT department as decisions on password ageing, the numbers of tries before a user is barred for forgetting a password and so on will vary from company to company.

The Version 3.00 software gives improvements in compliance but it will require the correct set-up of Windows NT security features to prohibit the use of Explorer to delete files and Notepad or Wordpad to carry out text editing. By making NTFS (New Technology Filing System) the disk format, your IT specialist can mark the **directories** for the measurement data, security and SOPs to be non-delete to protect these files from deletion. In the case of networked systems, it may be necessary to configure the sizer.ini file to automatically save the data to a central directory on your company's server.

Some files in the SizerS directory should receive special consideration:

Name	Size	Type	Modified
Data		File Folder	18/11/2002 14:46
Pages		File Folder	18/11/2002 14:46
Present		File Folder	18/11/2002 14:46
Programs		File Folder	18/11/2002 14:46
@&\$~\$&.\$@	1 KB	\$@ File	06/12/2002 14:51
CTL3D.DLL	27 KB	Application Extension	04/10/2002 14:27
HISTORY	2 KB	Text Document	02/12/2002 17:48
LOG100.SIZ	2 KB	SIZ File	04/10/2002 15:28
msyan.dll	53 KB	Application Extension	04/10/2002 15:16
PAINT	85 KB	Application	14/10/2002 08:37
present.dll	47 KB	Application Extension	04/10/2002 13:58
Sizer.cnt	10 KB	CNT File	04/10/2002 15:28
SIZER	673 KB	Application	18/10/2002 14:17
sizer	1,224 KB	Help File	25/04/2002 09:48
SIZER	9 KB	Configuration Settings	02/12/2002 14:29
smg	107 KB	Application	04/10/2002 13:58
smg	45 KB	Help File	04/10/2002 13:58
STD_RI	1 KB	Configuration Settings	04/10/2002 15:28
USR_RI	1 KB	Configuration Settings	04/10/2002 15:28

The **security config** file (which looks like a swearword because it is encrypted) cannot be secured using NT Security owing to the fact that the program reads it and writes to it for all users. It cannot be saved away to another directory – it needs to be located in the same directory as the sizer application.

However, it should be noted that if any attempt is made to delete or modify this file, a message box would appear asking for the software to be re-installed.

Re-installation of the software could only be done by the Administrator since a fraudster would not have the knowledge of other users passwords and permissions to be able to perform an undetectable re-installation and re-configuration of the security set up.

Other files that cannot be protected are:

Data files – these need to receive additional records as further measurements are completed.

***.inb files** - these have data about files last used.

malvern.piq – This keeps and maintains the queue for the SMG utility which calculates the light scattering matrices for new materials.

usr_ri.ini - this is modified if new particle types are added to the library of refractive indices. It can be protected after new particle/dispersant types have been added to the library.

sizer.ini and **user-name.ini** files - these need to be written to by the Administrator and the respective users of the files but write access to these files can be restricted to those individuals.

All other files can be protected (including programs, pages, bitmaps, reports, presentations) as follows:

- a) Open Windows Explorer, and then locate the file or folder for which you want to set permissions.
- b) Right-click the file or folder, click **Properties**, and then click the **Security** tab.
- c) Do one of the following:
To set up permissions for a new group or user, click **Add**. Type the name of the group or user you want to set permissions for using the format *domainname\name*, and then click **OK** to close the dialog box.
To change or remove permissions from an existing group or user, click the name of the group or user.
- d) In **Permissions**, click **Allow** or **Deny** for each permission you want to allow or deny, if necessary. Or, to remove the group or user from the permissions list, click **Remove**.

3) Support for Electronic Records/Electronic Signatures

Support for electronic records and electronic signatures (ER/ES) is provided by Adobe Acrobat technology.

This will require Adobe Acrobat version 5.0, or later, (to be purchased separately) to be installed.

Version 3.00 software has a new command: **Set-up - ER/ES Settings** which allows a path to be selected where Portable Document Format (PDF) files may be saved.) See also "*Legacy Systems ER & ES Advice*" (See "References", below) which examines the requirements of 21 CFR 11 one by one and defines how they are met.

Of particular importance is the section reproduced below:

**“Primary Requirements for a compliant system.
General Requirements :**

- (a) *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*



The protection of the electronic records requires the user to implement some form of backup procedure to copy the records onto a long-term storage medium such as magnetic tape or CD-ROM. The Mastersizer software does not provide a solution for this requirement because each user has different requirements. Some may choose to back-up to a central data server using a network, others may prefer to back-up at the instrument using a Tape Streamer or a CD-Writer. Since the Mastersizer runs on Windows NT/2000™ all of these options are available from third parties. “

Your IT specialist should know what protocols will apply to your particular set-up. We regret that we are unable to give specific advice on how you should set up your IT system or configure your workstation owing to the widely differing protocols observed by different companies.

4) Installing Version 3.00 software.

If you are updating from an older version of the Mastersizer series software, you **MUST** do the following:

- a) Make a backup and archive copy of your application software.
- b) Copy the relevant directory and its contents (e.g. for an old S installation in the default directory - C:\SizerS) to a temporary location.
- c) Delete the directory.
- d) Install the software to the required location.
- e) Copy any files that are required (e.g. configuration, security, measurement) back to the installation directory from the temporary directory. Reboot the computer to make sure that nothing is running in the background.

4) Configuring the Security Settings.

The first job for the IT specialist will be to set up the administrator so that he/she cannot be locked out by accident. It is a good plan to set up several administrators to provide cover against the possible absence of a single administrator.

Note that the administrator will often not be a particle-sizing expert and may only be allowed to have the ability to set up users and groups and administer the security.

Do *Setup > Security*. This will give this dialogue:

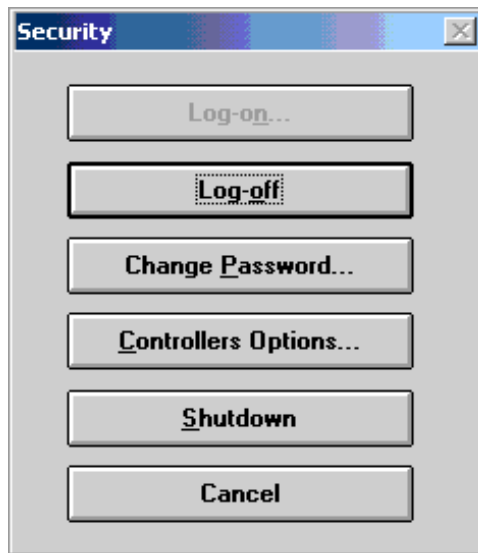


Figure 1 Security Configuration.

Select “Controllers options” to get this dialogue:

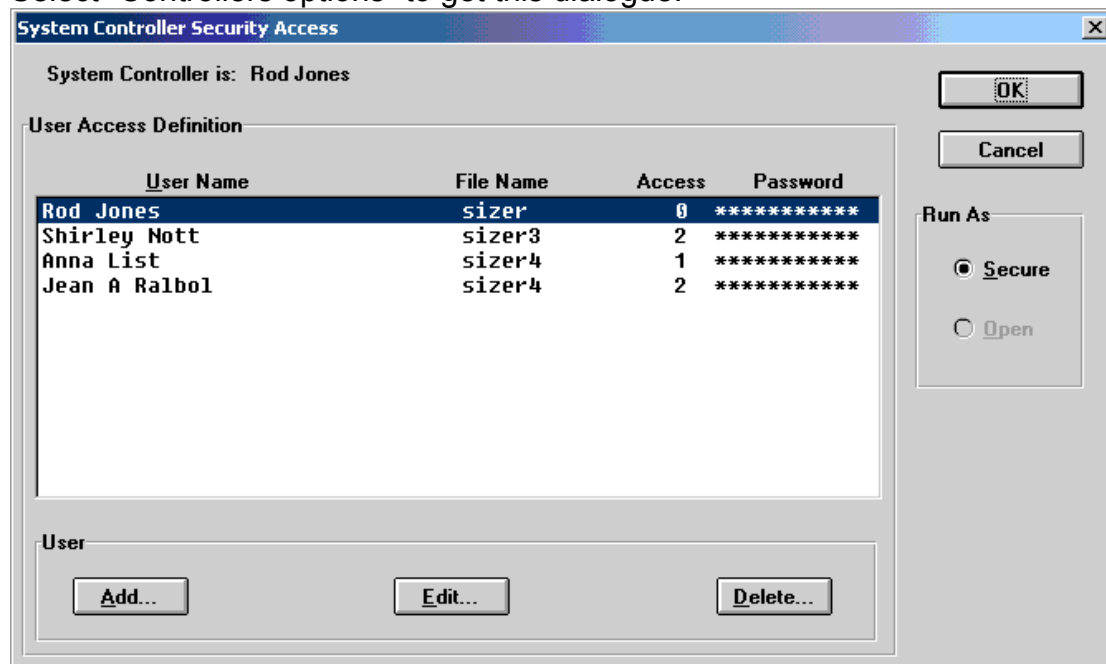


Figure 2. System Controller Security Access dialogue.

This dialogue allows the security controller to add new users and modify the details of existing users.

Note that 0 is the top access level while 2 is the least enabled.

To obtain the most precise control over the features that are accessible to different users, the controller can set each user to level 2 but then use a combination of assigned Basic macros and Easy Buttons to give them access to normally disabled commands. You will note that, in the above dialogue, a file name appears against each user. These files contain the individual user configurations including the macros and buttons that have been assigned to those users. These files should be protected using Windows NT Security Features as described in Section 2, above.

If the software is to be left running but unattended then the user should logoff using the Security command on the Set-up menu. New users then have to select the Logon command and enter their passwords to use the Mastersizer. Many companies will insist on continuous use checking so that users are automatically logged out after a given period of keyboard inactivity. This feature together with password ageing, password size and password history is available as an integral part of the Operating System Security – it is not offered as part of the Mastersizer software. To ensure that only authorised users access the software, it is recommended that the Mastersizer application is the **only** application installed on the computer.

If a second application is installed on the same workstation, it is possible that some of the users of the second application may not be authorised to use the Sizer application. However, they will have been enabled to bypass the Windows NT security and thus may have an opportunity to compromise the security of the Version 3.00 software.

5) Using Adobe Acrobat to produce Electronic Signatures.

Note that users requiring to use Adobe Acrobat® to produce Electronic Signatures will require the full PDF writer, not just the Reader which is available so freely on the Internet.

Adobe Acrobat Version 5 is not included in the price of the ER/ES feature key and should be purchased separately. The document “Legacy Systems ER/ES Advice” includes a description of the use of Adobe Acrobat to create Electronic Signatures.

Please note that the default installation procedure for Adobe Acrobat installs PDF Distiller rather than PDF Writer which is the utility used to create Electronic Signatures.

Insert the Adobe disk into the CD Rom drive and when the *Install* options are presented, select “*Custom*” and then select “*PDF Writer*”.

The PostScript printer driver should also be installed before using Acrobat to create Electronic Records. In addition to Adobe Acrobat, the Acrobat installer includes the Microsoft® PostScript 5 driver for Windows 2000, the AdobePS™ 4.5 (Windows 95/98/ME) and 5.2 (Windows NT®) printer drivers, as well as a set of Distiller® PostScript® Printer Description (PPD) files. Select a PPD file for the printer that you intend to use.

User Guide

MALVERN INSTRUMENTS

Reference:

(1) "Legacy Systems ER & ES Advice" The Requirements of 21 CFR Part 11 item-by-item with notes on the compliance of Version 3.00 software.

This document can be found in the *Info* directory on the Version 3.00 software CD Rom Part No. PSS0008-01.

URLs:

<http://www.Malvernevents.com> Powerpoint presentations with streaming audio for downloading on demand. Topics include a software tour of Version 3.00 software.

http://www.fda.gov/ora/compliance_ref/part11/frs/background/pt11finr.pdf

The FDA Guidance on 21 CFR Part 11.