

LogTag

Electronic Temperature Recorder



Digital Signatures User Guide

CONTENTS

Minimum System Requirements	3
1. Introduction	4
Figure1 : Diagram of system	5
2. Installing the software	6
2.1 Deployment	6
2.2 TCP/IP Port numbers	6
2.3 Installation	6
3. Configuring User Server Software.....	7
3.1 Enter User information	8
3.2 Enter Signature information.....	9
3.3 Assign Signatures to Users	10
3.4 Configuring Audit Events.....	11
3.5 Setting Administrator Password	13
3.6 Accessing password protected user server settings	14
4. Configuring Analyser Software.....	15
5. Adding a Digital Signature to a File	17
Requirements.....	17
Procedure.....	17
6. Event Viewer	20
6.1 Opening an Event Log File.....	20
6.2 Viewing the event list.....	21
6.3 Examined event content.....	23
Appendix A : FDA 21 CFR Part 11 introduction	24

NOTE:

This user guide assumes the use of

- *LogTag Analyser* software version 1.0 build 51
- *LogTag User Server* version 1.0 build 10.
- *LogTag Event Viewer* version 1.0 build 9

Information contained in this document regarding LogTag software use and the like is intended for suggestion only and may be superseded by updates.

No representation or warranty is given and no liability is assumed by LogTag Recorders with respect to the accuracy or use of such information, or infringement of patents or other intellectual property rights arising from such use or otherwise.

All rights reserved. © 2003 LogTag Recorders 6/2003 .

www.logtagrecorders.com

Minimum System Requirements

- Pentium II 233MHz processor
- 64Mb RAM
- 15Mb free disk space
- Windows 98,Me,2000,XP
- 1 free serial port or 1 free USB port with serial/USB converter or USB interface.
- 800 x 600 or better screen resolution.
- 256 colors or more recommended.

1. Introduction

The *Digital Signatures* support suite of software has been developed to support the *FDA title 21 CFR Part 11* standard. For further information see Appendix A in this user guide: “FDA 21 CFR Part 11 introduction”

In this standard *authenticated* users can *digitally sign* a set of recordings with a given set of *digital signatures* that has been allocated to those users.

A *Digital Signature* is registered with the recordings and contains information associated with the signing that clearly indicates all of the following:

- The printed name of the signer;
- The date and time when the signature was executed;
- The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Digital signatures remain permanently stored with the logger recordings file.

Authenticated Users are identified by unique *usernames* and *passwords*.

In addition, the standard requires that an Audit Event log of all activities is recorded.

LogTag uses a “client-server” approach for authenticating users and digital signatures.

The client software is *LogTag Analyser*.

This is the standard software for reading and configuring *LogTag* loggers and runs on computers that are reading, displaying and storing logger data.

The server software is *LogTag User Server*.

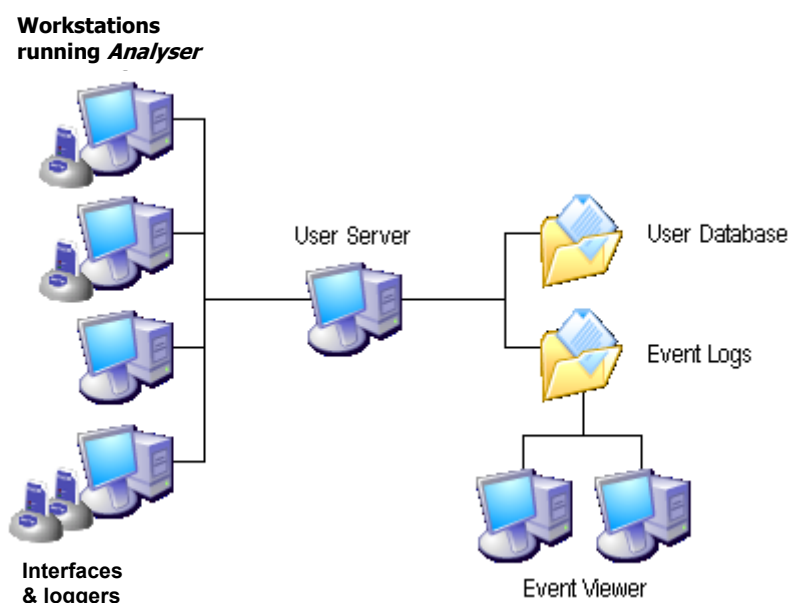
User Server is normally run on a server in a networked computer system but can be run on the same computer as *Analyser* provided security issues are observed.

The purpose of the *User Server* software is to provide access to the user & signature database to all appropriately configured *Analyser* clients and to maintain the *audit event log* of user activities.

An additional piece of software called the *Event Viewer* allows viewing of the audit events and is can be run on the same computer as *User Server* and/or other workstations provided those workstations have network access to the folders on the *user server* computer in which the event audit log files are stored.

Figure 1 overleaf shows the system diagrammatically.

Figure1 : Diagram of system



The *user server* concept allows user/password and event audit management across a LAN, WAN or even the Internet. It achieves this by using the TCP/IP network protocol (as used in the Internet) to transfer data (such as users/passwords and events) from/to a central location to *Analysers clients*.

This structure has several advantages over a simple file reference based system which include:-

- Higher security - users cannot connect to an unauthorized file (or server) without administrator privileges.
 - Users cannot directly access the user database to hack into the system without the attempts being recorded.
 - Able to optionally restrict Users ability to perform certain tasks with the Analyser software.
- Easy to manage – the user database is in one place.
- Ability to operate over a WAN (wide area network) or Internet. This provides the possibility of the user server concept to have a central server running that serves user passwords and manages event audits from anywhere (i.e. even from another country). A large organization can therefore have a single *user server* running (such as at head office) and provide the user server functions to office branches throughout the country (or even the World) provided the offices are connected to the Internet.
- All event audit logs that are generated are stored in a central location (normally on the same computer as is running *user server*)– this is a very real advantage particularly in large organizations when faced with either internal or FDA audits.

2. Installing the software

2.1 Deployment

Software deployment depends on the network structure on the installation site. Ideally, the *user server* software would be installed on a server within the site's network. This could be either a physical machine within the same building or a machine sitting at head office or the organization's IT department which is connected to the company's WAN, LAN or through the internet. Alternatively, if only one workstation is to be used to access logger data and either there is no LAN or network structure then the *user server* software can be installed on that computer also. It is advised that the *administrator password function* (see section 3.5) is enabled in *user server* to protect the system from unauthorized tampering.

2.2 TCP/IP Port numbers

Because the *Analyser & User Server* use TCP/IP network communications for data exchange a TCP /IP port number needs to be selected that is not used by other software in the network.

TCP/IP port numbers range from 1 to 65535. The system administrator should select a port number that best suits the system. We suggest port numbers of 768 or 2000.

2.3 Installation

Note: For Windows 2000 and XP you may need to be logged in as the "administrator" to install the software. All software is supplied as a single executable self installing file.

Step 1: Install *User Server*

- Select the computer/server to run the *user server*.
- Install the *User Server* software onto this computer by double clicking on user server self installing file.
- Configure *user server* as detailed in section 3.

Step 2: Install *Analyzer* software.

- Install *Analyzer* on required workstations.
- Setup *Analyzer* according to requirements and the *Analyzer User Guide*.
- Setup *Analyzer* for connection to *user server* as defined in Section 4 of this guide.

Step 3: Install the *Event Viewer* software

- Select computers/workstations that will require *Event Viewer* and install *Event Viewer* by double clicking on event viewer self installing file.
- Ensure that the event log location on the *user server* computer (as detailed in section 3.4) is shared out to workstations (with the appropriate permissions) installed with *Event Viewer*.

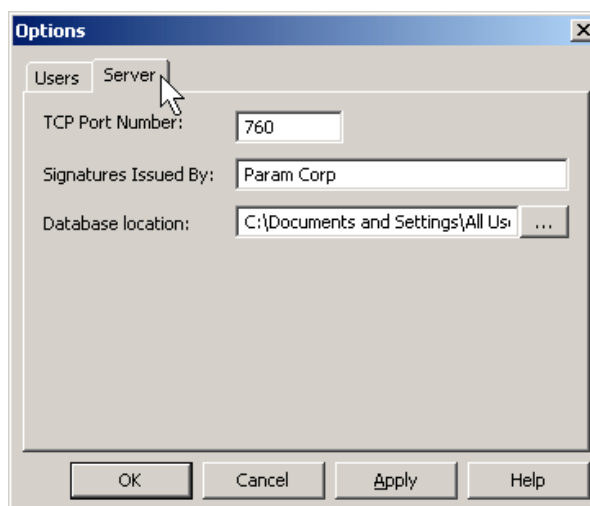
3. Configuring User Server Software.


- Once installed, the *User Server* Software the server software installs itself into the *Windows system tray*.



Figure 2: User Server when not active in the System Tray

- Double click on the system tray icon to open the user server software.
- Enter administration user name & password if required (not required on first time configuration)
- Click on the *View* menu then *Options*
- Click on the *Server* tab and set the TCP port number. Choose a TCP port for connection to the network. Note you cannot select a port which is already in use including 8, 21, 25, 80, 8080. (on many networks TCP port number 760 is OK)



 **NOTE:** Firewalls in the network may need to be configured to pass this TCP port number. At no time will the User Server software send information to an external network destination, so the privacy of your information is maintained.

- Information entered in the *Signatures Issued By* box will be included in every digital signature written to data files.
- Once User Server has been configured with access to a valid TCP Port Number, the User Server software will automatically start servicing user requests.



Figure 3: User Server when active in the System Tray

3.1 Enter User information

- Click on **Users** menu and select **New**.
- Enter User information and password as prompted.
- Tick option boxes as appropriate for the user concerned.

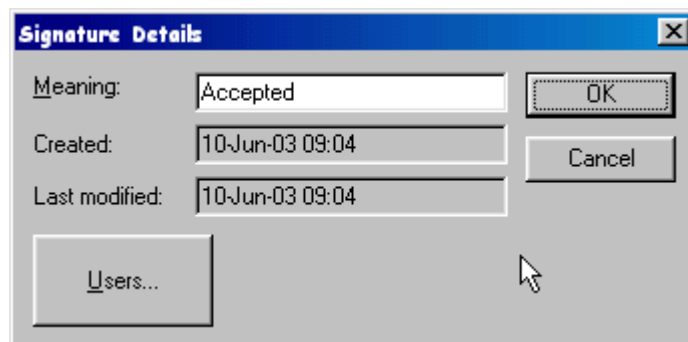
The screenshot shows a 'User Details' dialog box with the following fields and options:

- Username: fsmith
- Full name: Fred Smith
- Description: QA Manager
- E-Mail: fred@pharma.com
- Password: *****
- Confirm Password: *****
- Account disabled
- User can change password
- User must change password on next logon
- Buttons: Signatures..., Permissions..., Logoff
- Buttons: Add, Cancel

- The *Signatures* button allows association of existing signatures types to this user.
- The *Permissions* button allows configuration of what actions and resources a particular user has access to.
- Click **Add** to add this user.
- The User name will appear on the main screen.
- When you have finished adding users, click the Close button.
- User information can be modified by highlighting the User name, then clicking on **Users** and **Edit**.

3.2 Enter Signature information

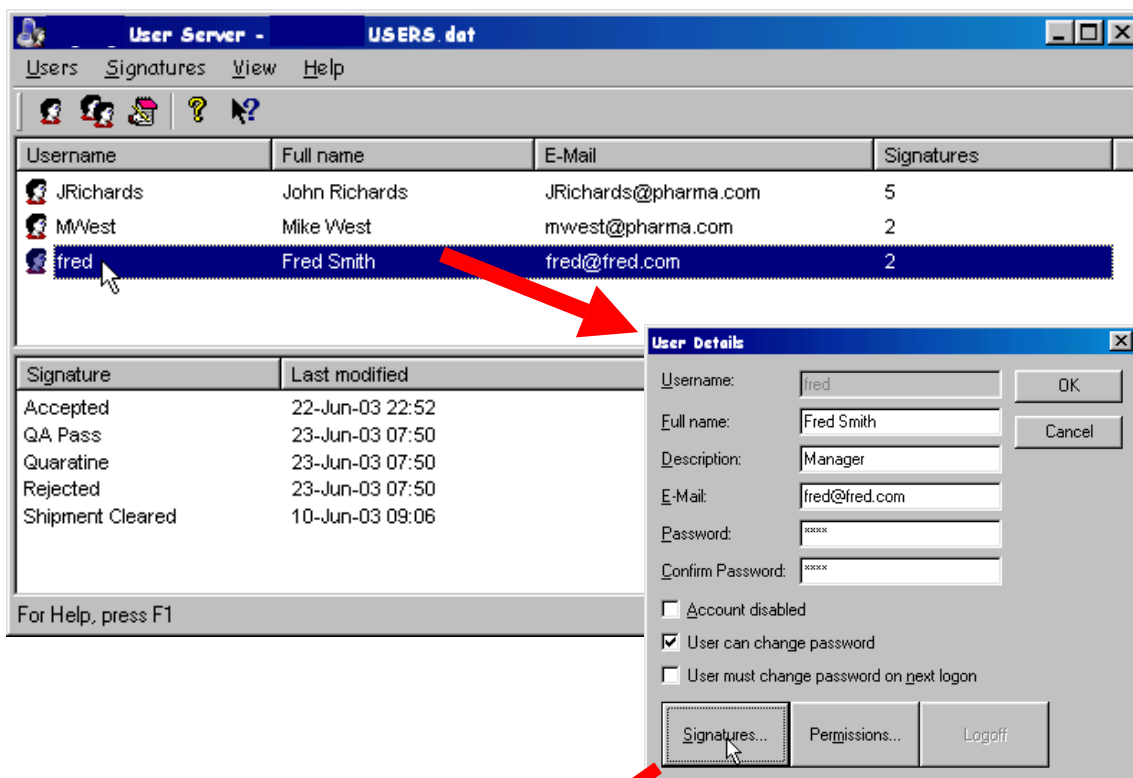
- Click on **Signatures** menu and select **new**.
- Enter signatures in **Meaning** box. For example, "Accepted", "Rejected", "Quarantine".



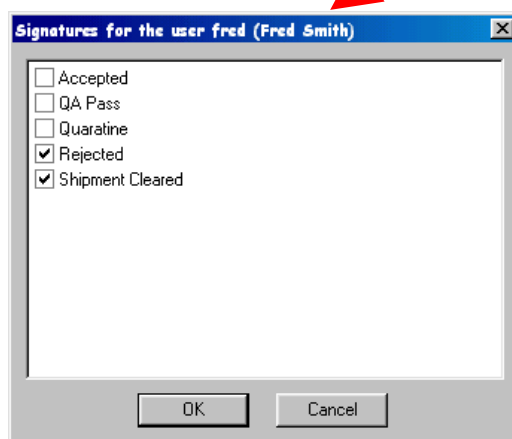
- The Users button will allow you to add or remove Users permission to utilize this digital signature.
- A list of signatures defined will appear in the lower half of the main screen
- Signatures can be modified by highlighting the signature, then clicking on "Signatures" and "Edit".

3.3 Assign Signatures to Users

- Double click on a user or highlight user and click on **Users** menu then **Edit**.



- In User window, click on **Signature** button.

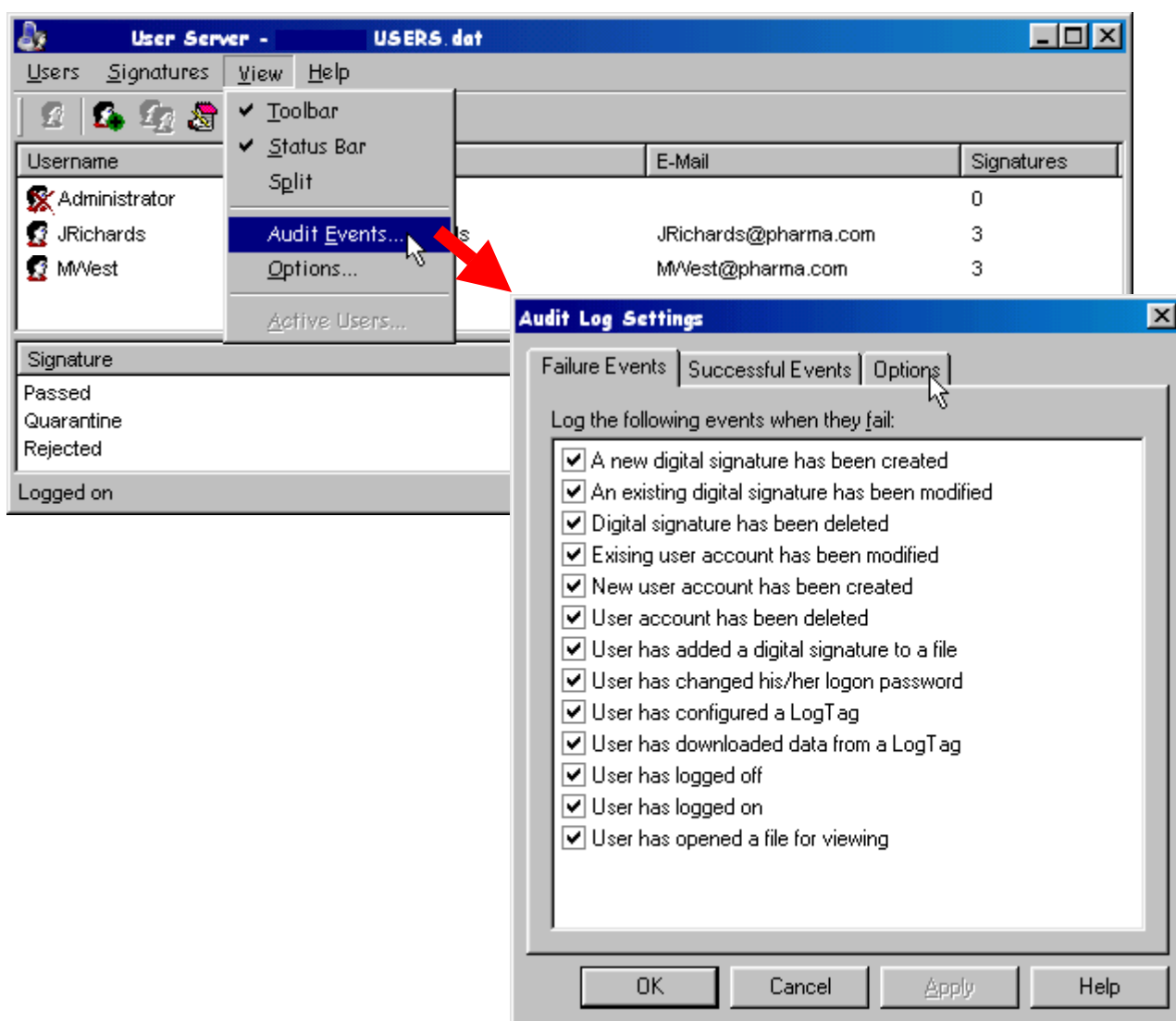


- Enter a tick against the list of authorised signatures for that user.
- Click on **OK**. The number of signatures for which that user is authorised will appear on the main screen against the user name, and the number of authorised users will be shown against that signature.

3.4 Configuring Audit Events

Audit Events track all user actions as a time & date stamped event which are stored in an *event file*. The actions to be logged and the event log files location can be configured by accessing the *Audit Events* settings.

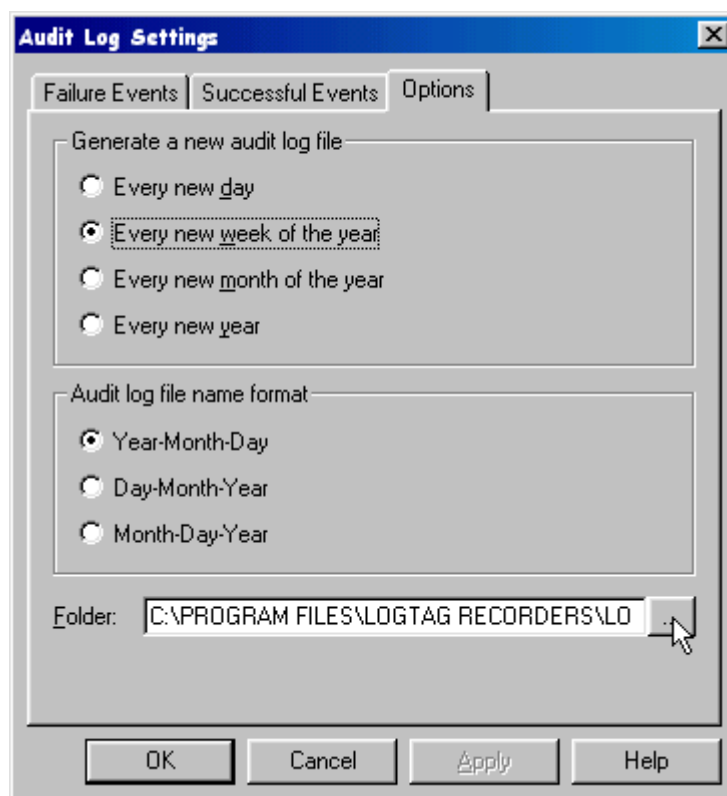
Click on the **View** menu, **Audit Events** to open the **Audit Log Settings...**



Failure Events are a list of possible action *failures* that are recorded in the event audit log. Un-tick actions that are not required to be recorded. (all are active by default)


Click on the **Successful Events** tab. **Successful Events** are a list of possible action *successes* that are recorded. Un-tick actions that are not required to be recorded. (all are active by default)

Click on the *Options* tab to access the Audit Event file settings configuration ..



The Event audit log can be configured to generate a new file daily, weekly, monthly or yearly.

Folder defines the location of the event audit files – this location can be changed to suit the installation site requirements and also needs to be known so that the user can locate the files with the *event viewer*.

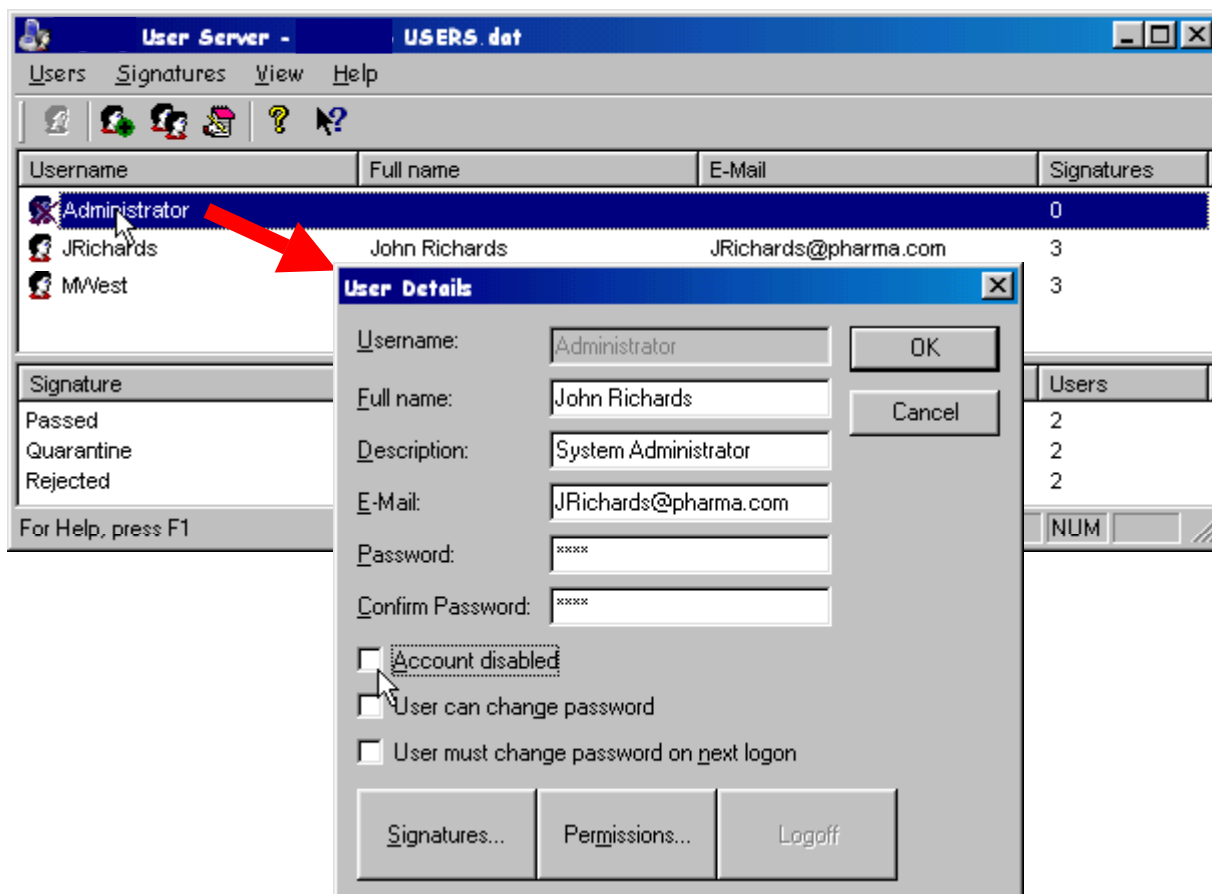
Click on  to view or change the Audit Events folder location.

The Event Viewer software will not delete any audit log files, so it is up to the administrator to ensure there is enough disk space available for the audit log files.


3.5 Setting Administrator Password

The administrator user is a special user that can be configured to restrict access to the user server database and configuration.

To configure the administrator password, double click on the administrator user.



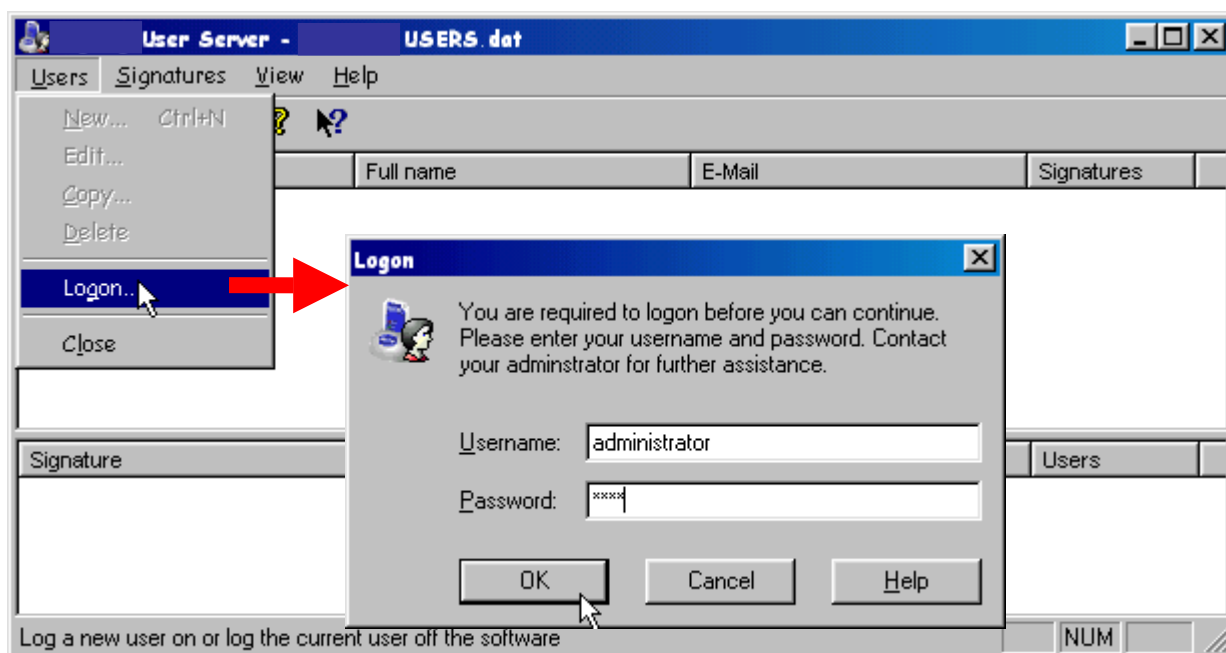
1. Enter the full name of the administrator etc and the password.
2. Un-tick **Account Disabled** to activate. Click OK.
3. The *users.dat* screen reappears.

 If you wish to leave *user server* in a password protected state then remember to logoff the administrator. (Select **Users** then **Logoff User**)

It is not possible to delete the Administrator account. If you no longer want the *Administrator* account to be active, repeat the above steps with the exception of placing a tick in the "Account disabled" field.

3.6 Accessing password protected user server settings

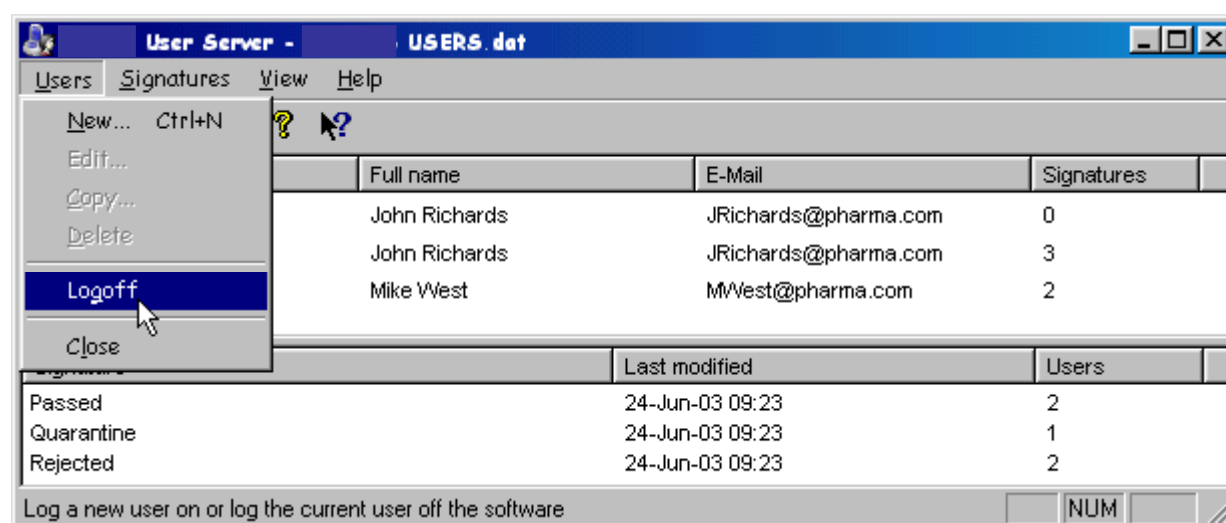
Double click the *user server* system tray icon to open the user server window. If the user server is password protected then blank entries are displayed and you will need to log on as the *administrator* to gain access to the *user server* database and settings. Click **Users**, **Logon** and enter the username “administrator” and the previously configured password. (see section 3.5 for further information)).




If the username and password are correct then the user server window will then display the current user database settings and the associated menus will become accessible.



Once you have completed working with *user server* remember to logoff the Administrator account. (Select **Users** then **Logoff User**).

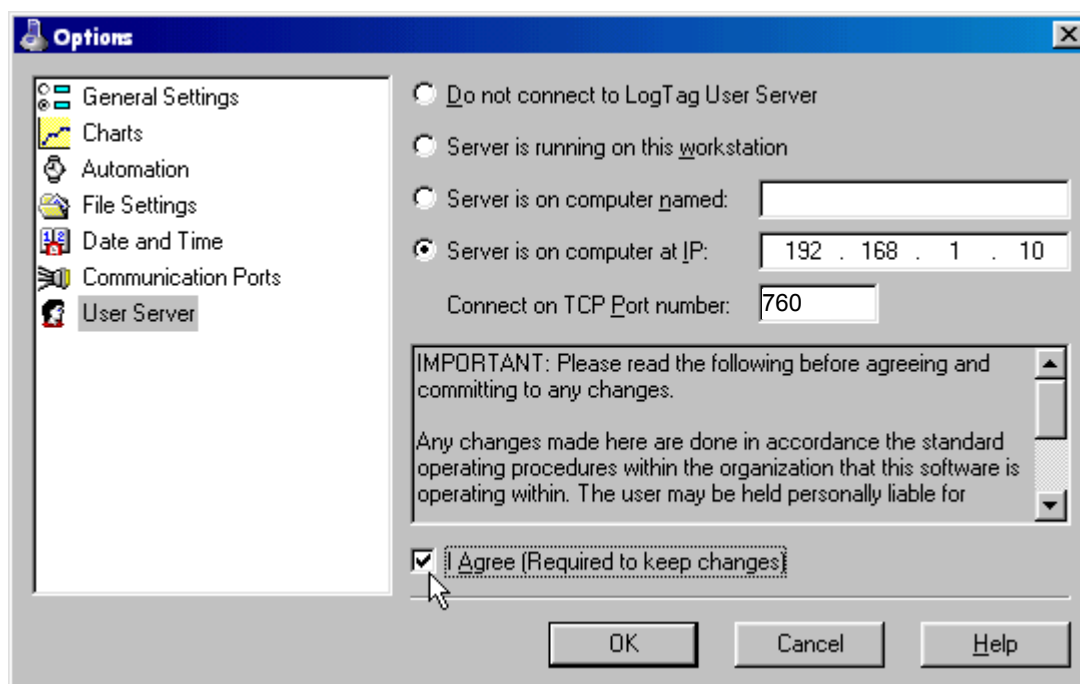


Once logged off the blank user server screen will re-appear and click  to minimise it back to the system tray.

4. Configuring Analyser Software.

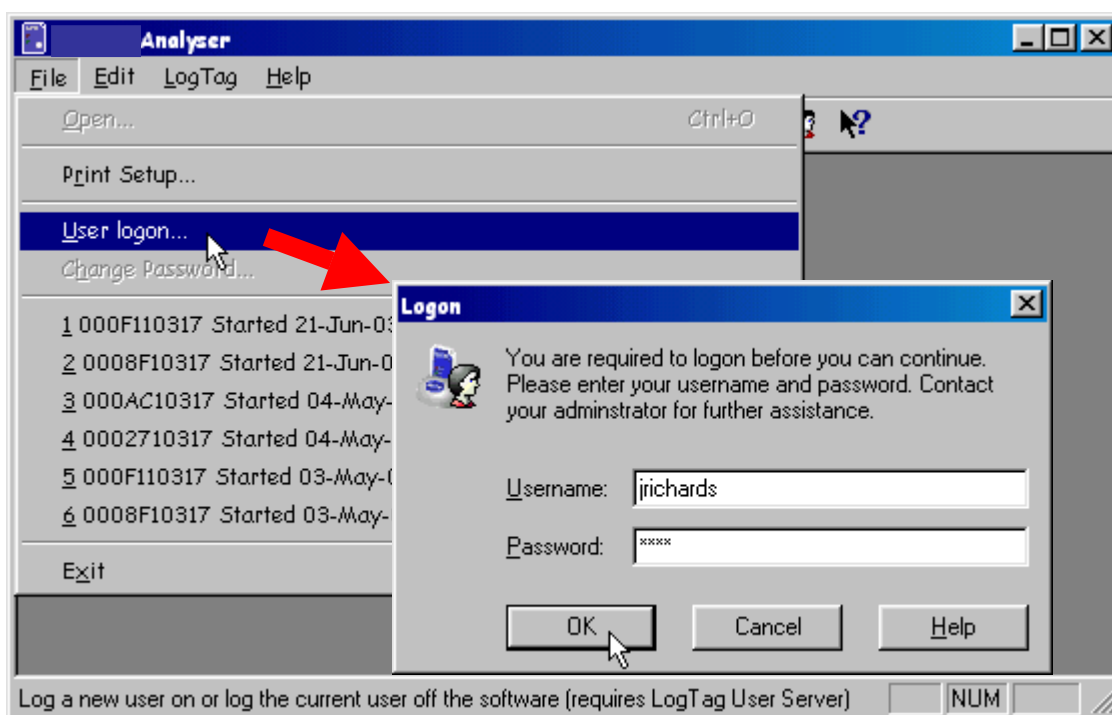
- Start *Analyser* and click on “**Edit**” menu then “**Options**”
- From Options menu displayed, select **User Server**
- Choose the option that best matches the set up of your network.

An example is shown below:-



- Click on **Server is running on this workstation** if the user server and *Analyser* are running on the same workstation.
 - Click on **Server is on a computer named** if the user server is running on a server or another workstation with a known computer name.
 - Click on **Server is on a computer IP** if the user server is running on a server or another workstation with a fixed and known IP address. (useful for WAN or internet deployments)
 - Enter the **TCP Port Number** – must be the same as configured in *user server*.
-
- Read the notice and if you agree with what is stated, tick the **I Agree** box to allow changes to be saved and used.
 - Click on the **OK** button to close the dialog and activate the new settings.

- Before proceeding, the user must log on by clicking on the **File** menu then selecting “**User logon**” or by clicking on the logon toolbar button.

**NOTE:**

- To add Digital signatures to files:
 - The Analyser software must be configured to connect to User Server (see above) and able to connect to the User Server.
 - A user must be successfully logged on to the Analyser software.
 - The user must have been authorised to add digital signatures (see section 3.3 for more information).
- Once the TCP network connection is set, it is not necessary to restart the software to activate the change.
- Workstations must have the network protocol TCP/IP installed prior to attempting to set the connection to User Server.

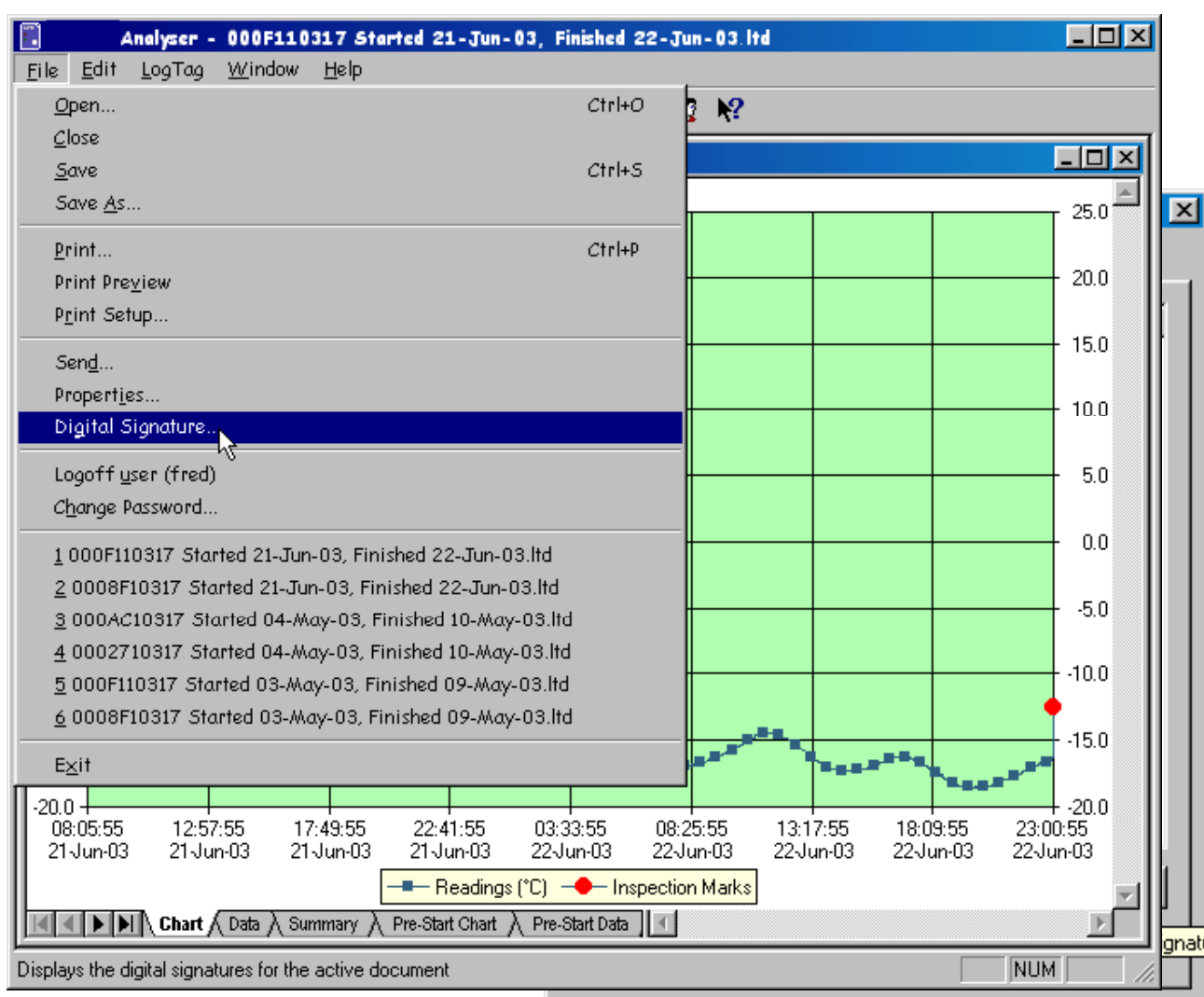
5. Adding a Digital Signature to a File

Requirements

- *User Server* software, configured correctly and running on workstation or server as defined in *user server configuration*.
- *Analyser* software configured to access *user server*.

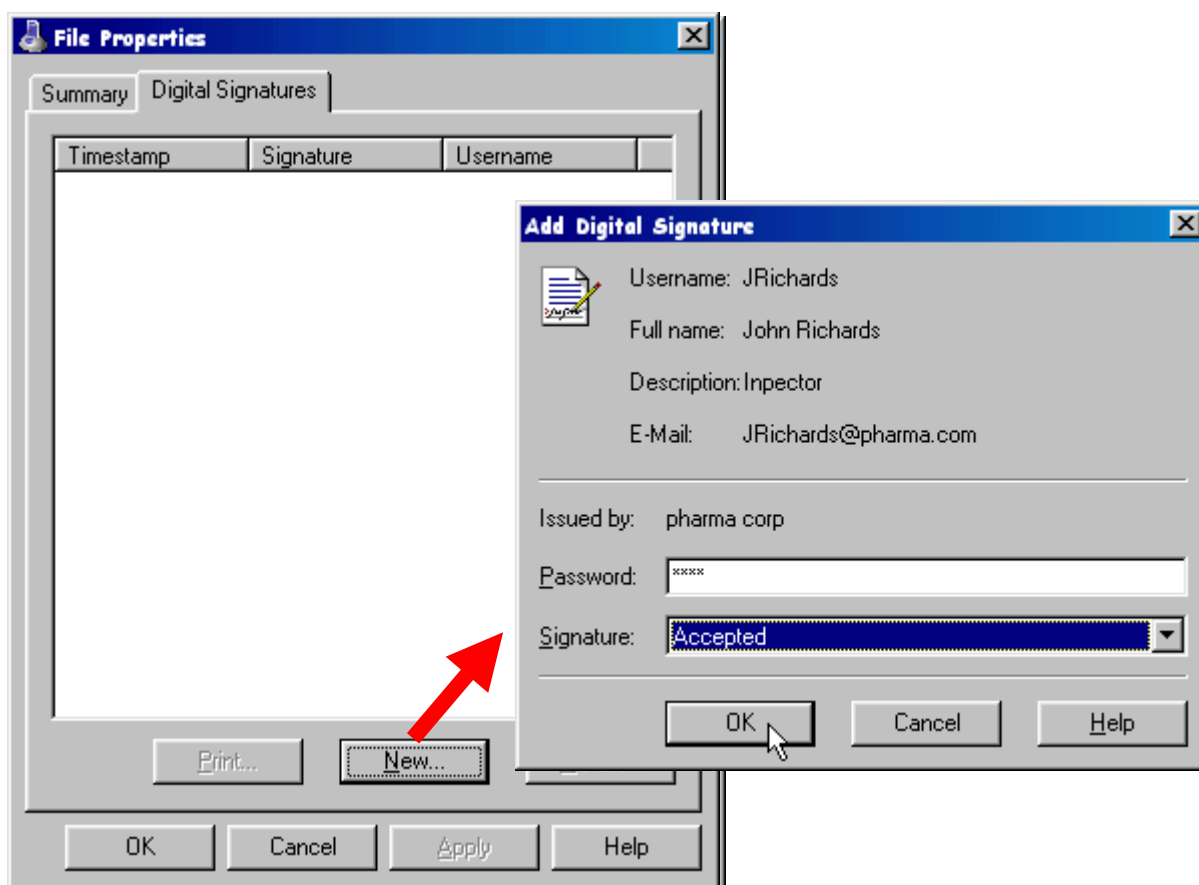
Procedure

- Start *Analyser* software (if not already running) – user is prompted for a username & password.
- Enter User Name and Password, then click OK. If logon is successful, the blank *Analyser* screen will be displayed and the *Analyser* menus become accessible.
- Click on “File” and select the file to be signed from the menu.
- Click on “File” and select “Digital Signature” from the menu.



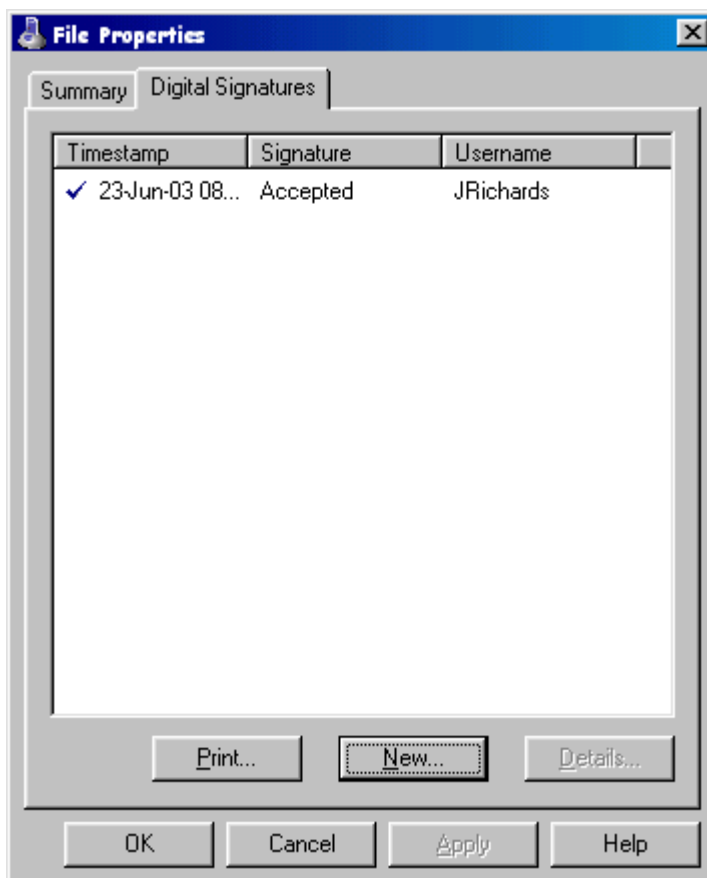
- A File Properties window will be displayed. Click on the ‘Digital Signatures’ tab.

- Click on the 'New' button and enter the user's password.
- The **Signature** drop down box provides a list of authorised signatures for the user. Select the signature required.



- The user will be asked to confirm that a digital signature should be added to the file. Click the **Yes** button to permanently digitally sign the file. Each file is capable of storing many digital signatures.
- Click OK to close the File Properties window.

A list of the digital signatures included in a file can be viewed by clicking on “File” then selecting Digital Signature. The File Properties window opens. Click on the Digital Signatures tab to display the signatures. These signatures are permanently included in the file.



Click on **Print** to print the details of the digital signatures to a specified printer.

6. Event Viewer

The *Event Viewer* is a tool that allows display of the events generated by *user server*. The software is normally installed and run on the same computer that is running *user server* however it can be operated on any computer provided it can gain access to the folder that contains the audit event log files that the *user server* software generates. The Event Viewer software will only display the contents of the audit event log files and does not and cannot make any modifications to the files.

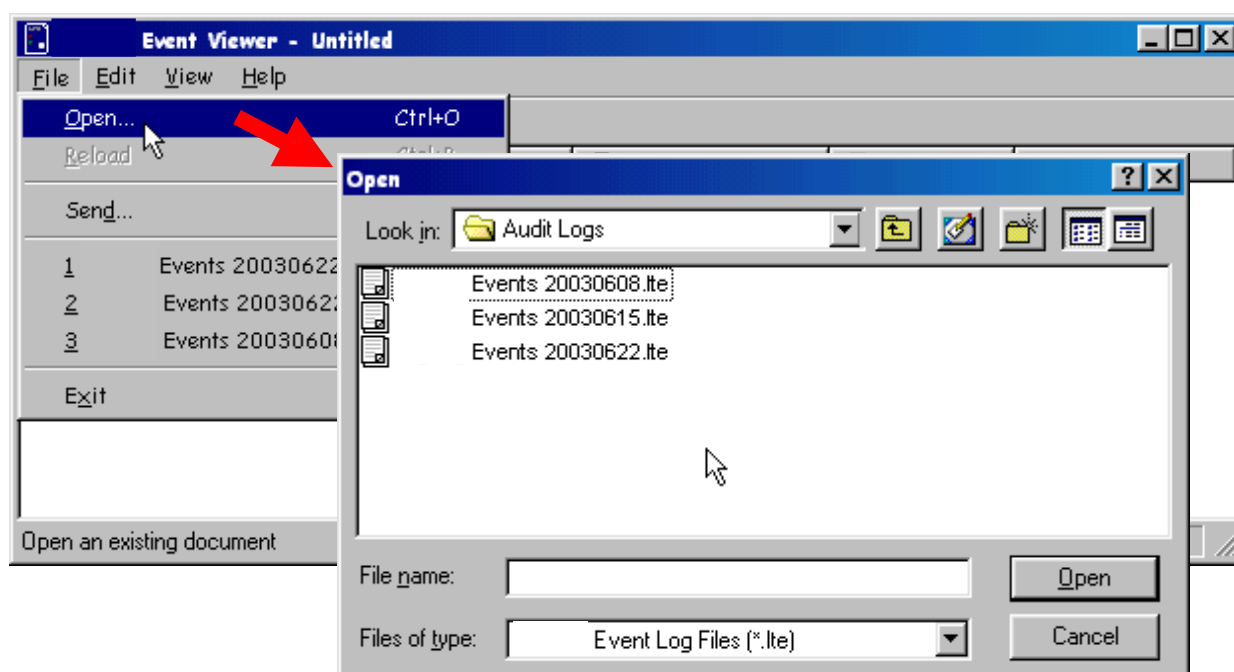
The event logs are stored in files with date coded unique filenames either daily, weekly, monthly or yearly at a file location as defined in the *user server* configuration.

To start *event viewer* either double click the desktop icon or run from the *Programs* list off the start menu.

6.1 Opening an Event Log File

In order to be able to display events an event file must be selected and opened. Click **File, Open** and browse to the event folder location defined in *User Server* configuration.

If the Event viewer is running on a different computer to the one running *user server* then the drive and directory on the *user server* computer in which the event log files are being stored needs to be shared out to the network, preferably with only 'Read only' access.

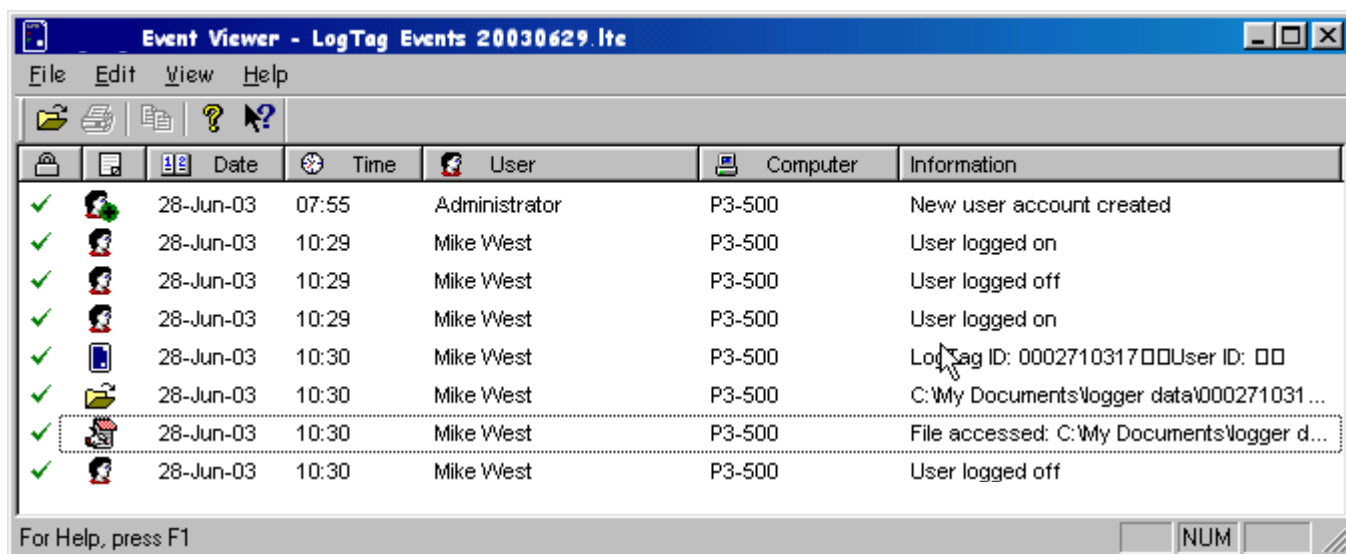


Double click on the file to open or select and click **Open**.

6.2 Viewing the event list

Once a given event file has been opened, the events recorded are then displayed as a scrollable list.

An example of an event log shown by Event Viewer is illustrated below:-



The Event Viewer displays the following information about each logged event:











Table 1: Event Viewer Column definitions

Column	Content
	Indicates whether or not the event entry has been tampered with within the file. ✓ Indicates the entry has not been modified ✗ Indicates the entry has been externally modified and may not be genuine information
	Symbol identifying type of event
Date	Date the event occurred
Time	Time the event occurred
User	The name of the user that generated the event
Computer	The name of the computer the event was generated on
Information	Summary information about the event

If desired, click on a specific column heading to sort the list by that content.

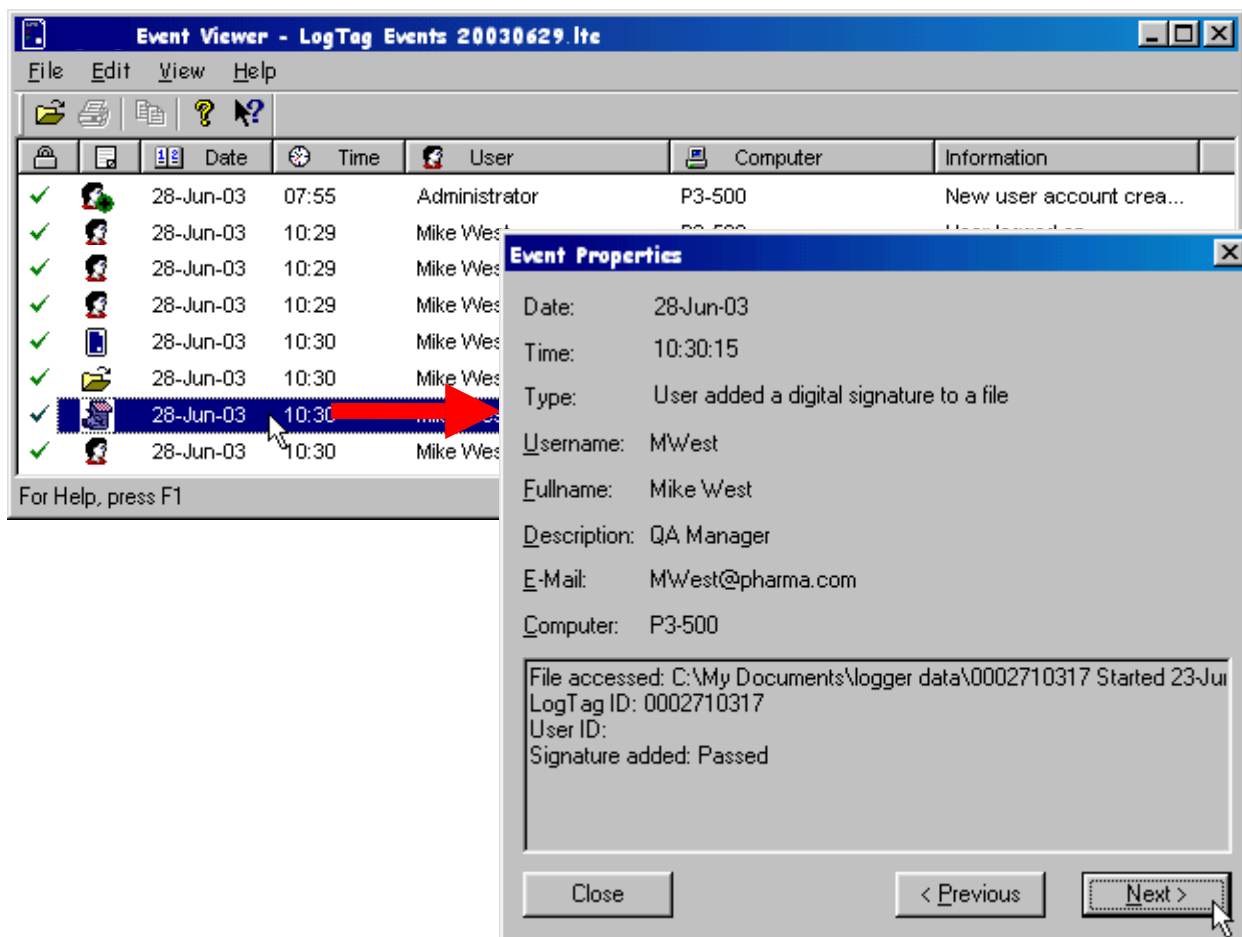
Event types are identified by different icons in the left hand column (🗂️):-

Table 2: Event Viewer Event Symbol definitions

Icon	Meaning
	User accessed and opened a file for viewing
	User activity (logged on/off etc)
	User added a digital signature to a file
	Logger downloaded or configured
	New user account created
	User account modified
	User account deleted
	New digital signature created
	Digital signature modified
	Digital signature deleted

6.3 Examined event content

Double click on an event to examine the event in detail:-



Click *Next* or *Previous* to view the next and previous events in the list.

Appendix A : FDA 21 CFR Part 11 introduction

1. What is 21 CFR Part 11?

Full name of standard is *Title 21 Code of Federal Regulations, Part 11*.

Title 21 includes regulations for Food and Drugs. Chapter 1 (parts 1 through 1299) includes the U.S. Food and Drug Administration (FDA) part of the U.S. Department of Health and Human Services.

Part 11 established the criteria under which electronic records and signatures will be considered equivalent to paper records and handwritten signatures in manufacturing processes regulated by the FDA.

FDA-regulated industries, such as Bio-Pharmaceutical (Human and Veterinary), Personal Care Products, Medical Devices and Food and Beverage, are required to document and acknowledge conditions and events at several points of each manufacturing and distribution process to insure exact procedures are followed and to produce consistent and repeatable products every time. Signed documents must be reviewed, securely stored and available for review by the FDA. The reviewing of these records was time consuming and required manual searches of the manufacturing information. 21 CFR Part 11 was issued to make this practice more accurate, timely and easier for everyone involved.

2. What are the benefits of electronic signatures and record keeping?

The benefits of electronic signatures and record keeping are significant. It increases the speed of information exchange and advanced searching capabilities, reduces the cost of record keeping storage space, increases data integration and trending information, improves product quality and consistency, and reduces vulnerability of signature fraud and report misfiling.

3. When was 21 CFR Part 11 instituted?

The rule was proposed in August, 1994, with a final ruling in March, 1997. It became effective in August, 1997, and the FDA started an aggressive enforcement in January, 2000.