LogTag Recorders

Digital Signatures

User Guide

Revision 1.2 build 1, Document Revision 1.12

Published 31. Octover 2011

Contents

Copyright iii

Disclaimer iii

Introduction 1

System Requirements....3

Installing the software 4

Deployment....4
Networked Installations....4
Stand-Alone Installations....4
Installation....5
Step 1 - Install User Server....5
Step 2: Install LogTag® Analyzer software....5
Step 3: Install the Event Viewer software....5
Installing User Server as a service....6

Configuring LogTag User Server Software 8

Initial Set-up....8
Enter User information....11
Enter Signature information....12
Assign Signatures to Users....13
Configuring Audit Events....14
Failure Events....15
Successful Events....16
Audit Log Settings....17
Setting the Administrator Password....18
Accessing password protected LogTag User Server settings....19

Configuring LogTag® Analyzer Software. 21

Adding a Digital Signature to a LogTag® file 23

Requirements....23
Procedure....23

LogTag® Event Viewer 26

Opening an Event Log File....26
Viewing the event list....27
Examining the Event Content....29

Appendix A : FDA 21 CFR Part 11 introduction 30

Copyright

Disclaimer

LogTag User Server is a utility that allows system administrators to deploy a user login system for LogTag® Temperature and Humidity & Temperature recorders, so the system complies with the requirements published by the US Food & Drug Administration. Familiarity with system administration procedures is a prerequisite for using this software, and as a consequence LogTag Recorders will release this utility only to distributors and selected end clients who are familiar with the use of LogTag® products and have the required IT administration capabilities.

This user guide assumes the use of:

- LogTag User Server version 1.1 build 2
- LogTag® Event viewer v1.1 build 1 or later
- LogTag® Analyzer software v2.2 build 17 or later

Introduction

The Digital Signatures support suite of software has been developed to support the FDA 21 CFR Part 11 standard (see "Appendix A : FDA 21 CFR Part 11 introduction" on page 30). In this standard, authenticated users can digitally sign a set of recordings with a given set of digital signatures 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 user names 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® Analyzer.
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.
LogTag User Server is normally run on a server in a networked computer system but can be run on the same computer as LogTag® Analyzer, provided security issues are observed.

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

The ***Event Viewer*** is a utility program that allows viewing of the audit events. It can be run on any computer, as long as it has access to the location of the event audit log files within the network.

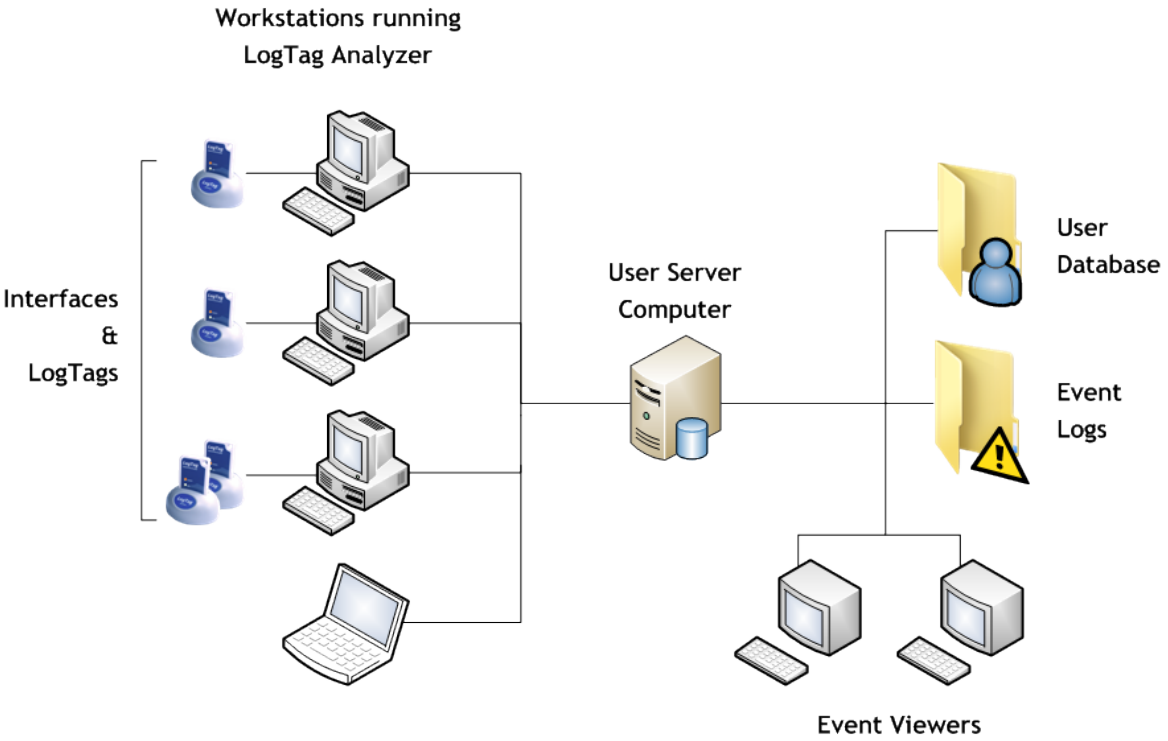


Figure 1: System Diagram

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 to transfer data (such as users/passwords and events) between a central location and LogTag® Analyzer 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.
  - Users' ability to perform certain tasks with the Analyzer software can optionally be restricted.
- Easy to manage – the user database is in one place.
- Ability to operate over a LAN, WAN 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 LogTag 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 generated are stored in a central location (normally on the same computer as is running LogTag User Server) – this is a very real advantage particularly in large organizations when faced with either internal or FDA audits.

System Requirements

These are the minimum specifications for a computer intended to operate LogTag User Server:

- PC capable of running Windows XP or later, or Windows 2003 Server or later
- 15MB free disk space
- Internet Explorer 5.0 or later
- 1 available serial port and/or 1 available USB port, depending on purchased interface
- 1024 x 768, or higher, screen resolution.
- 256 screen colours

Recommended Specifications are as follows:

- Processor equivalent to Pentium IV or later
- 512MB of available RAM
- Internet Explorer 6.0 or later
- 65535 (16bit), or more, screen colours.

Installing the software

Deployment

Software deployment depends on the network structure on the installation site.

Networked Installations

Typically the LogTag User Server would be installed on a server within the site's network. This server can physically be located anywhere, provided client computers can connect to it through company's WAN, LAN or through the Internet.

Stand-Alone Installations

Alternatively, if only one workstation is to be used to access logger data and there is no LAN or network structure, the LogTag User Server can be installed on that computer also. It is strongly recommended the *administrator password function* (Setting the Administrator Password (on page 18)) is enabled in LogTag User Server to protect the integrity of the system and to prevent unauthorized tampering.

Installation

Note: In operating systems from Windows 2000 onward you will need to be logged in as the "administrator" to install the software. All software is supplied as a single executable self installing file called "ltserver_10r14.exe" or similar.

Step 1 - Install User Server

- Select the computer/server on which to run LogTag User Server.
- Install the LogTag User Server software onto this computer by executing the downloaded file, which will be named "ltserver_10r14.exe" or similar.
- Perform the initial set-up as described in Initial Set-up on page 8.
- Configure LogTag User Server as detailed in Configuring User Server Software on page 8.

Step 2: Install LogTag® Analyzer software

- Install LogTag® Analyzer on required workstations. You can also perform a network installation.
- Setup LogTag® Analyzer according to requirements and the LogTag® Analyzer User Guide.
- Setup LogTag® Analyzer for connection to LogTag User Server.

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 LogTag User Server computer (Configuring Audit Events (see page 14)) is shared out to workstations (with the appropriate permissions) installed with Event Viewer.

Installing User Server as a service

If User Server is installed on a network server, typically no user is logged on when the system is running so there is less vulnerability to security breaches. Although LogTag® User Server installs itself so it can run in the taskbar, it cannot natively run without login credentials.

You can, however, install User Server as a service with the help of the Windows Resource Toolkit. This procedure needs to be performed **after** User Server has been installed on the network server computer.

Note: This technique is directed towards experienced network professionals who are familiar with the procedures required. It involves editing the registry. If you do not have experience with network administration or editing the registry please do not attempt this procedure. Due to the variety of operating systems and configurations LogTag Recorders will only be able to provide very limited support.

Note: This procedure has been written for and been tested with Windows Small Business Server 2003 R2. Similar techniques are available for other server operating systems, please consult the Microsoft Knowledge Base for further information regarding your specific OS.

Note: Some workstation operating systems do not provide the tools necessary to perform this procedure. Installation of User Server on a workstation computer as a service must be left to an experienced IT professional; LogTag Recorders recommend the use of a dedicated server computer for User Server.

1. Install the Windows Resource Tool kit for your operating system. Note the installation path to the "tools" folder. Some operating systems have this resource kit already installed. In this case search for the two executable files "Instsrv.exe" and "Srvany.exe". Note the location of these files.
2. Start a command prompt.
3. Type `"path\INSTSRV.EXE" LTUserServer "path\SRVANY.EXE"` where path is the drive and directory of the Windows Resource Kit, e.g. `"C:\Program Files\Windows Resource Kits\Tools\INSTSRV.EXE" LTUserServer "C:\Program Files\Windows Resource Kits\Tools\SRVANY.EXE"`. This will create a service called LTUserServer, but you are free to choose a different name. Please note it is not sufficient to navigate to the Resource kit directory, both `INSTSRV.EXE` and `SRVANY.EXE` must be called with the full drive and path name. You will receive a message that the service has been created successfully.
4. Start the registry editor and back up the registry.
5. Check the following key has been created:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LTUserServer`

   With the key highlighted, select the **EDIT** menu and click **NEW** then **KEY**. Type `Parameters` into the key and press **ENTER**.

   Highlight the Parameters key, select the **EDIT** menu and click **NEW** then **STRING VALUE**. Type `Application` into the value name and press **ENTER**.

6 Double click the Application value. Into the Value Data field, enter the full path name to the LogTag® User Server executable, e.g.

`"C:\Program Files\LogTag Recorders\LogTag User\LogTag Users.exe"`. Click **OK**.

7 If you wish, you can add a description to the service which will be displayed in the services console. To do this, highlight the LTUserServer key, select the **EDIT** menu and click **NEW** then **STRING VALUE**. Type `Description` into the value name. Double click the Description value. Into the Value Data field, enter the description you would like to see displayed, e.g. `Administers logon data for LogTag User Server.`

8 Close the registry editor. The service is configured to run automatically by default. If you wish to change this setting, you can do so via the Services console.

If at some stage you wish to remove this service, stop the service from the Services console, then open a command prompt and type `"path\INSTSRV.EXE" LTUserServer REMOVE` where path is the drive and directory of the Windows Resource Kit as described above.

Note: The User Server service is now owned by the SYSTEM. If you wish to change any settings in User Server, you need to do the following:
1. Stop the service from the Services console.
2. Open User Server by double clicking on the desktop icon or through the Programs shortcut.
3. Log on and make the desired changes.
4. Close the User Server program and exit the program from the taskbar.
5. Start the service from the Services console.

Configuring LogTag User Server Software

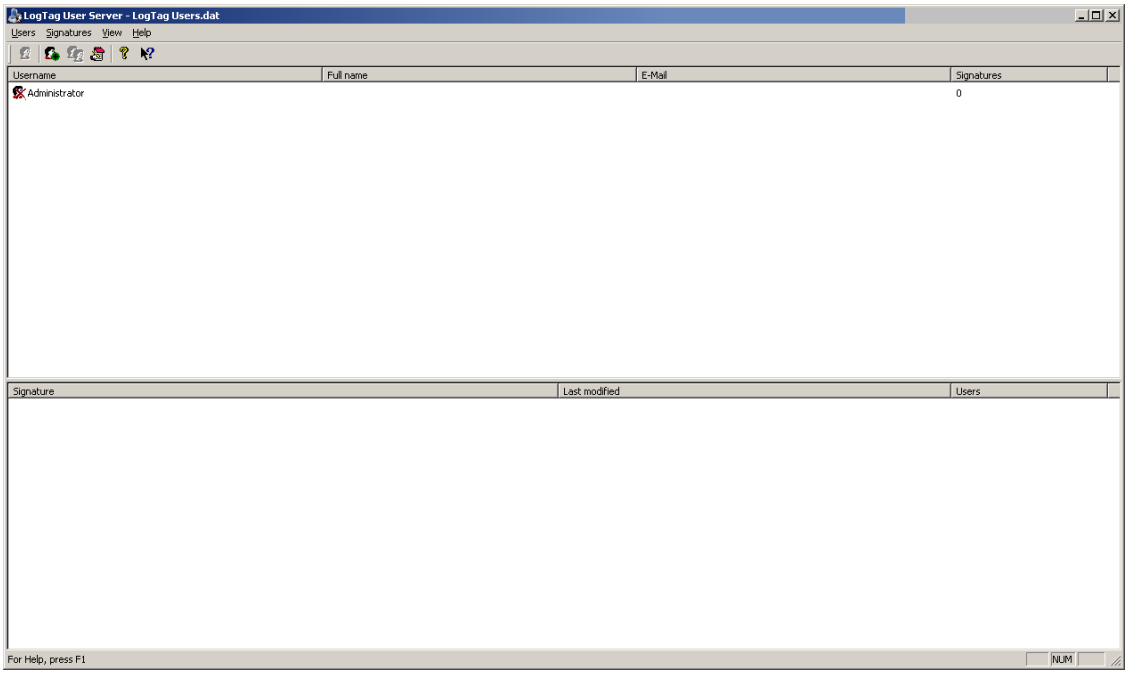
Initial Set-up

Once started, LogTag User Server installs itself into the Windows system tray. Until the initial set-up is completed, the software is inactive.

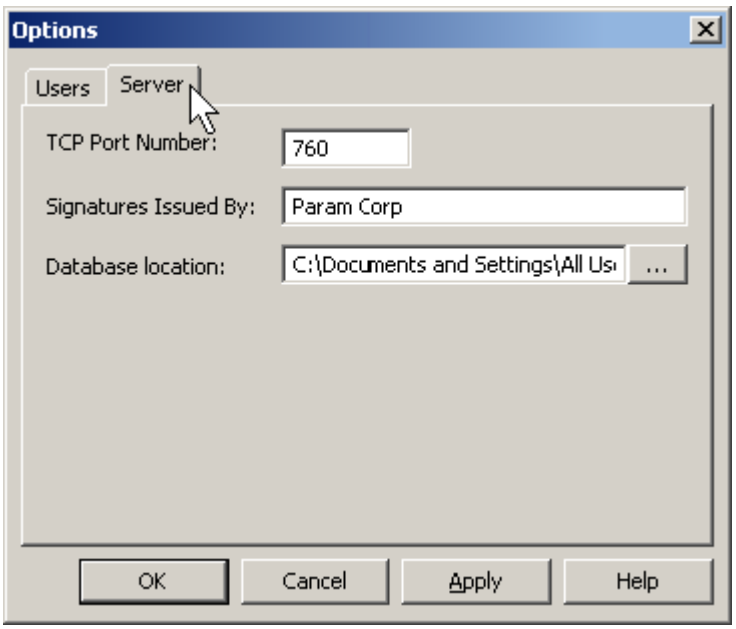
Figure 2: User Server when not active in the System Tray

To complete the initial set-up, you must enter basic configuration and connection data:

- Double click on the system tray icon to open the LogTag User Server software. You will see the LogTag User Server main screen:



- Click on the **VIEW** menu then **OPTIONS** and then click on the **SERVER** tab:



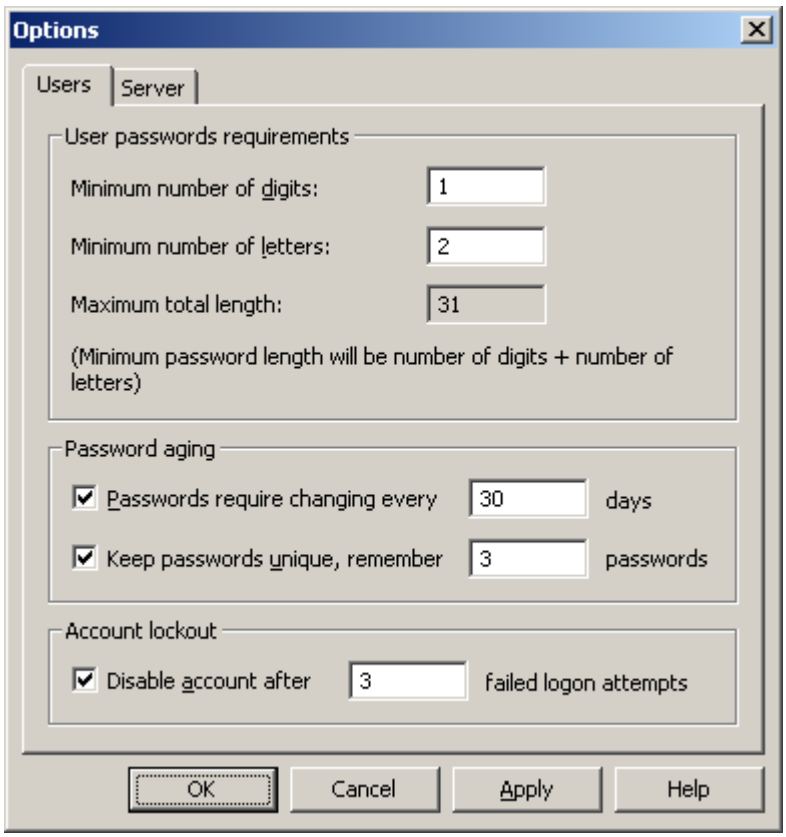
Set following parameters:

- 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. TCP/IP port numbers range from 1 to 65535. System administrator can select a port number that best suits the IT system.

This is the minimum setup required. The remaining items have default values, but it is recommended these defaults are changed to suit the specific requirements of your organisation.

- Signatures issued by; Enter the company information that you wish to appear in the signatures field of the file properties in LogTag® Data files. This information will be included in every digital signature written to data files.
- Database location; Select the storage location where the database files will be stored, which hold the user information. This can be different from the location of the log files, but please note that the folder must be accessible to the User Server software at all times, so a network location should not be chosen.

- Click on the **VIEW** menu then **OPTIONS** and then click on the **USERS** tab:



- User password requirements; you can set the number of digits and letters a password must contain as a minimum. You can set either value to 0. In this case an empty password would also be allowed. The minimum password length is the sum of the minimum number of digits and letters. In the above example therefore a password has to be at least 3 characters long. The default values are 0.
- Password aging; this determines how often passwords must be changed. If you want users to be able to keep their password indefinitely, remove the check mark in the appropriate tick box. You can also prevent users from re-using the same password when they are requested to change. In this case, place a check mark in the tick box to keep passwords unique and enter how many unique passwords are required before they can be re-used. By default these options are disabled.
- Account lockout; This defines the behaviour when users enter incorrect passwords. If you wish to limit the number of logon attempts with an incorrect password to stop "trial and error" logon attempts, place a check mark in this tick box and enter the maximum number of logon attempts with an incorrect password. By default this option is disabled.

NOTE: Firewalls in the network may need to be configured to pass this TCP port number. The User Server software will not send information to an external network destination unless requested by an external LogTag® Analyzer installation, so the privacy of your information is maintained.

Once LogTag User Server has been configured with access to a valid TCP Port Number, it will automatically start servicing user requests.

Figure 3: User Server when active in the System Tray

If at any time you wish to make changes to any of the data, you must enter administration user name & password, which is not required on first time configuration.

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 **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.

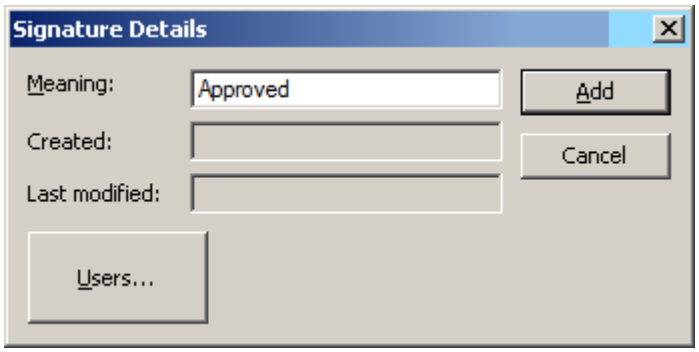
When you have finished adding users, click the **CLOSE** button.

User information can be modified by highlighting the User name, then clicking on **USERS** and **EDIT.**

Note: The user name and password are **not** linked to the Windows logon credentials. If a user has a Windows logon, but no User Server logon, they will not be able to log onto LogTag User Server software. A user without a Windows logon, but with a User Server logon will be able to log onto LogTag User Server software on any PC were a valid Windows logon has been provided.

Enter Signature information

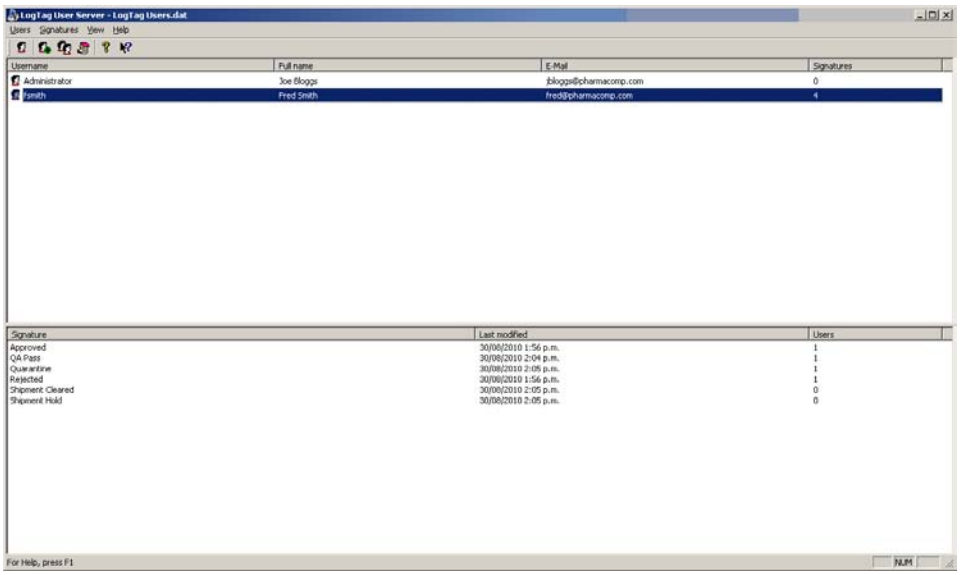
- Click on **SIGNATURES** menu and select **NEW.**



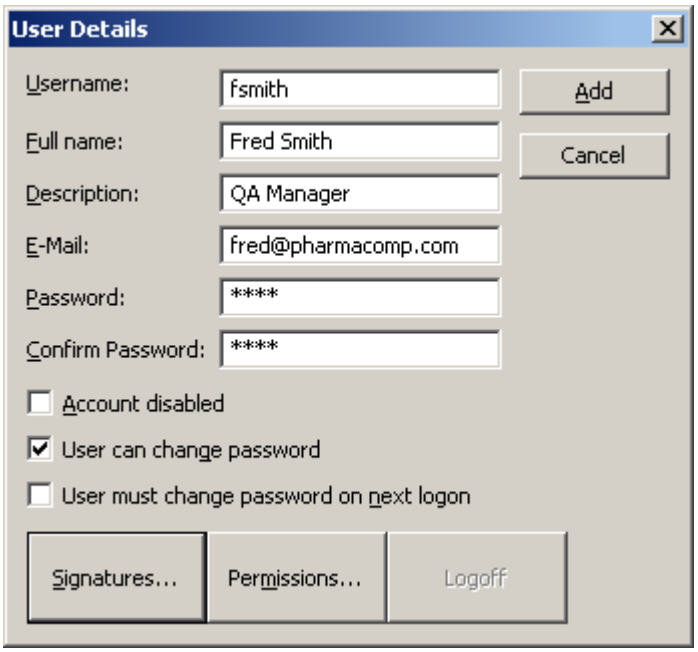
- Enter the signature description in the **MEANING** box. For example, “Approved”, ”Rejected”, ”Quarantine”.
- The **USERS** button will allow you to add or remove Users permission to utilize this digital signature.
- A list of signatures defined will appear in the lower half of the main screen
- Signatures can be modified by highlighting the signature, then clicking on **SIGNATURES** and **EDIT.**

Assign Signatures to Users

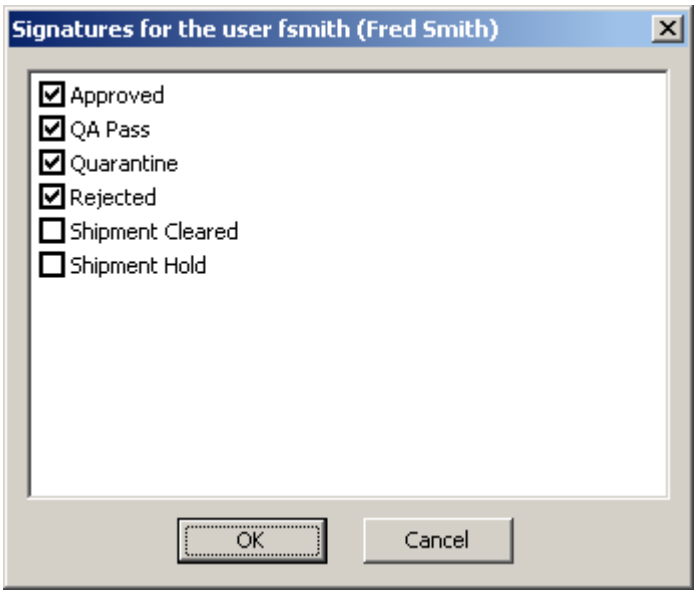
Double click on a user or highlight user and click on **USERS** menu then **EDIT.**



The User Details Screen is displayed.



In User window, click on the **SIGNATURE** button.



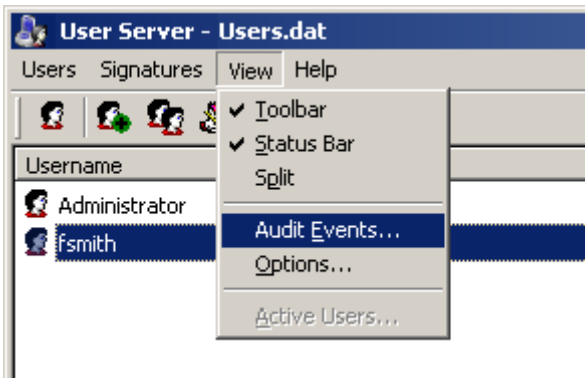
Enter a tick against each signature you want this user to be authorised to apply.

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.

Configuring Audit Events

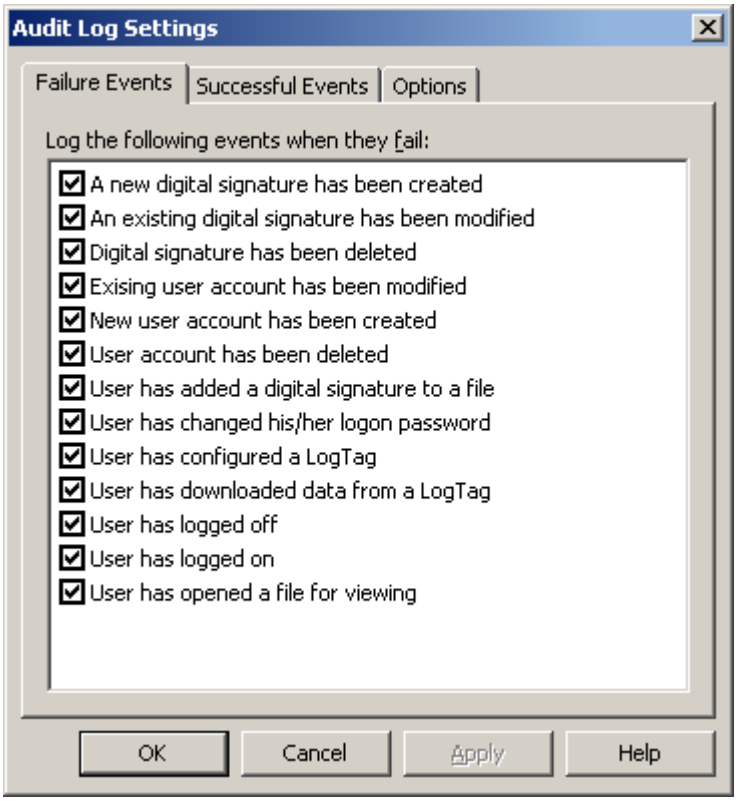
Audit Events track all user actions as a time & date stamped event which are stored in an event file (see page 26). The actions to be logged and the event log files location can be configured by accessing the Audit Events settings Event Viewer (see "LogTag® Event Viewer" on page 26).

Click on the **VIEW** menu, **AUDIT EVENTS** to open the Audit Log Settings.



The Audit log window will appear.

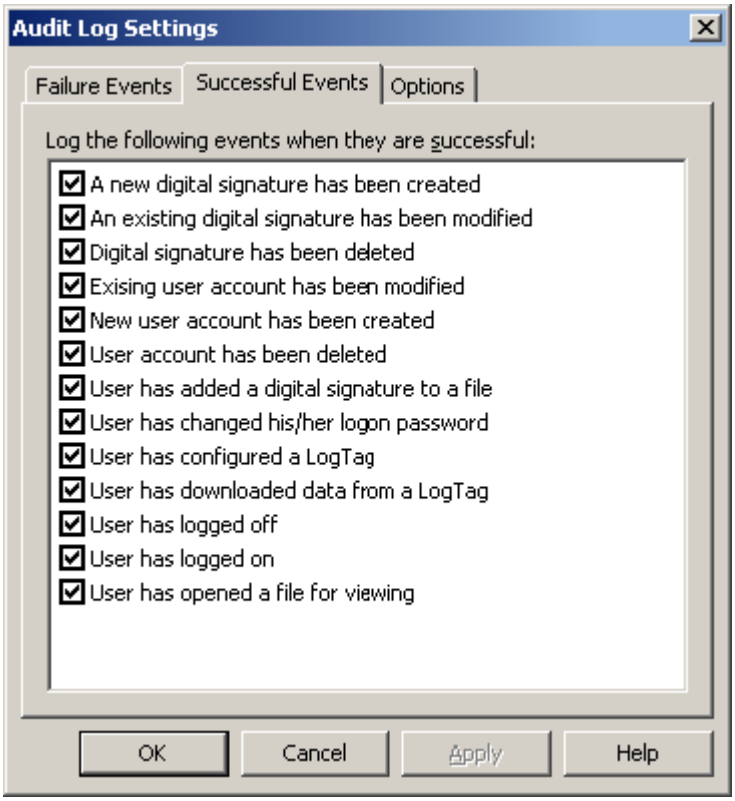
Failure Events



These 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.

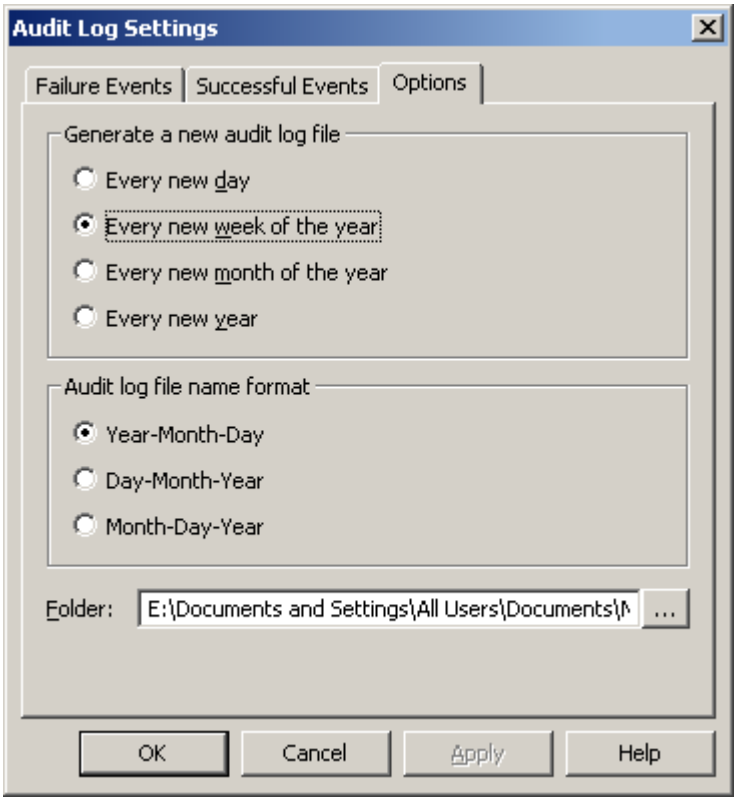
Successful Events



A list with the same entries is also displayed here, however this time it displays the 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

Audit Log Settings

The Event audit log can be configured to generate a new file daily, weekly, monthly or yearly. You can also determine the make up of the file name generated for this period.



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 located the files with the ***event viewer.***

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

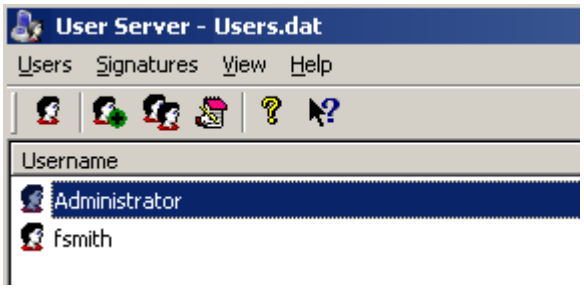
The default location for a Windows XP/2000 operating system is:-

`C:\Documents and Settings\All Users\Documents\Shared Documents\My LogTag Data\Audit Logs`

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.

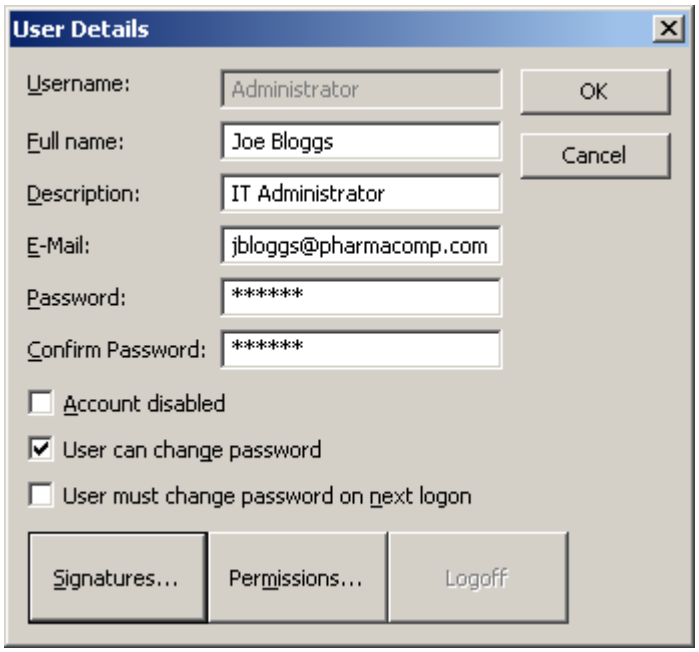
Setting the Administrator Password

The administrator user is a special user who can be configured to restrict access to the user server database and configuration.To configure the administrator password, double click on the administrator user.



The User Detail screen for the Administrator is displayed:

- Enter the full name of the administrator etc and the password
- Un-tick **ACCOUNT DISABLED** to activate
- Change the password settings as desired



- Click OK.

The standard user screen re-appears.

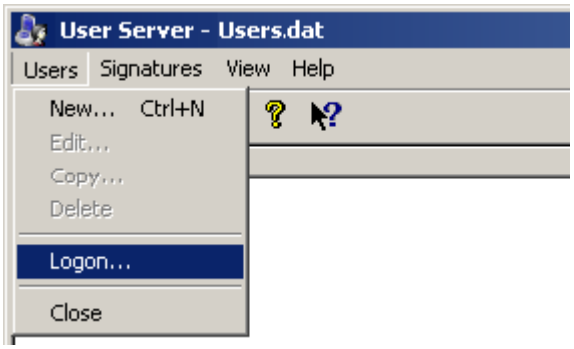
If you wish to leave LogTag User Server in a password protected state you need to logoff the administrator. (Select **USERS** then **LOGOFF USER**)

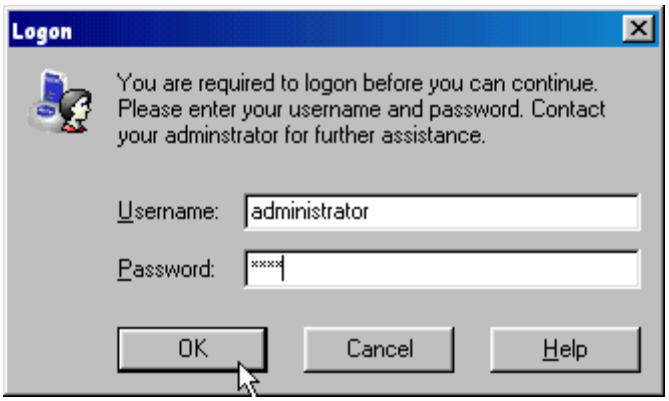
It is not possible to delete the Administrator account. If you no longer want the Administrator account to be active, repeat the above steps with the exception of placing a tick in the “Account disabled” field.

Accessing password protected LogTag User Server settings

Double click the ***user server*** system tray icon to open the user server window.

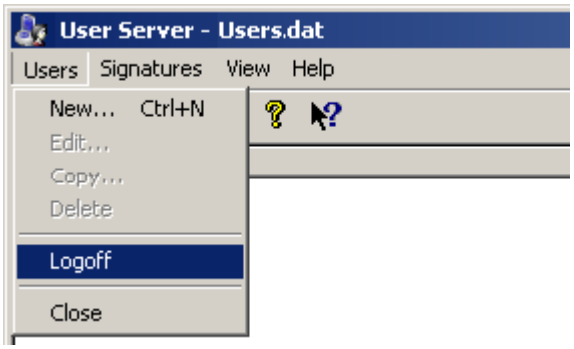
If the user server is password protected then blank entries are displayed and you will need to log on as the administrator to gain access to the user server database and settings. Click **USERS**, **LOGON** and enter the username "administrator" and the previously configured password (Setting the Administrator Password (on page 18)).





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 LogTag User Server remember to logoff the Administrator account by selecting **USERS** then **LOGOFF USER**.

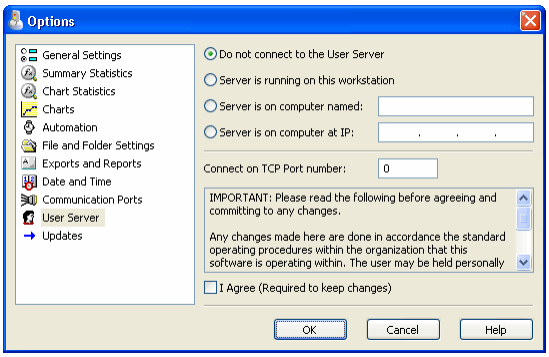


Once logged off the blank user server screen will re-appear. Click  to minimise it back to the system tray.

Configuring LogTag® Analyzer Software.

Start LogTag® Analyzer and click on the **EDIT** menu, then **OPTIONS.**

From Options menu displayed, select **USER SERVER**



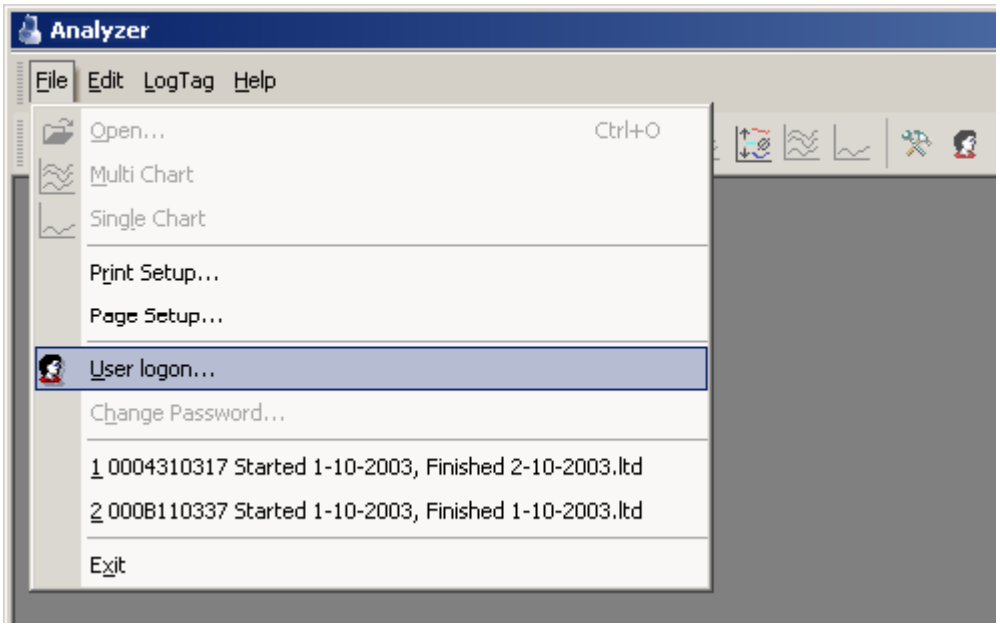
Choose the option that best matches the set up of your network.

- Click on Server is running on this workstation if LogTag User Server and LogTag® Analyzer are running on the same workstation.
- Click on Server is on a computer named if LogTag User Server is running on a server or another workstation with a known computer name.
- Click on Server is on a computer IP if LogTag User Server is running on a server or another workstation with a fixed and known IP address. (useful for WAN or internet deployments).

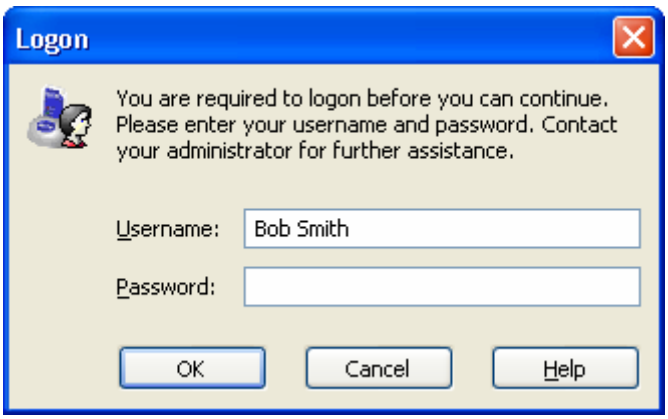
Enter the TCP Port Number – this must be the same as configured in LogTag User Server.

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.



The logon dialogue will be displayed:



To add Digital signatures to files:

- LogTag® Analyzer must be configured to connect to LogTag User Server(see above). You will receive an error message if a connection cannot be established. Once the TCP network connection is set, it is not necessary to restart the software to activate the change.
- A user must be successfully logged on to LogTag® Analyzer.
- The user must have been authorised to add digital signatures (Enter User information on page).
- Workstations must have the network protocol TCP/IP installed prior to attempting to set the connection to LogTag User Server.

Adding a Digital Signature to a LogTag® file

Requirements

LogTag User Server software, configured correctly and running on workstation or server as defined in Configuring LogTag User Server Software on page 8.

LogTag® Analyzer software configured to access LogTag User Server.

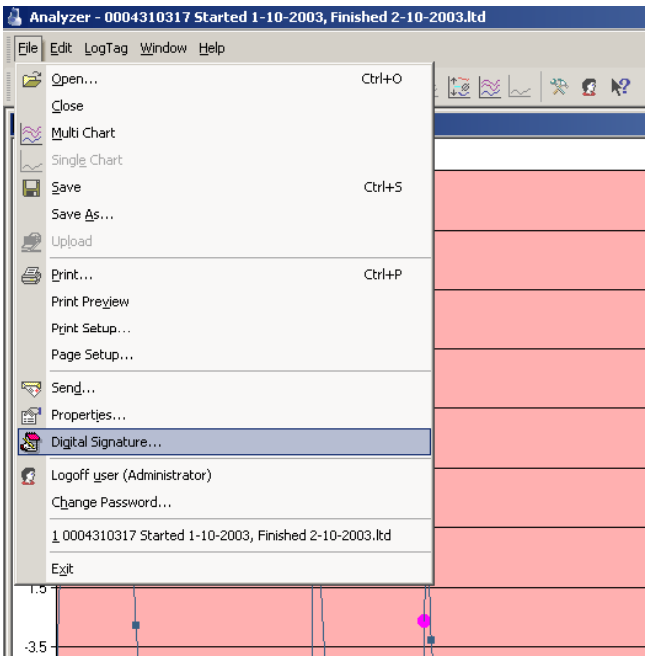
Procedure

Start LogTag® Analyzer software (if not already running) – user is prompted for a user name and password.

Enter User Name and Password, then click OK. If logon is successful, the standard Analyzer screen will be displayed with the menus accessible according to the user's permission settings.

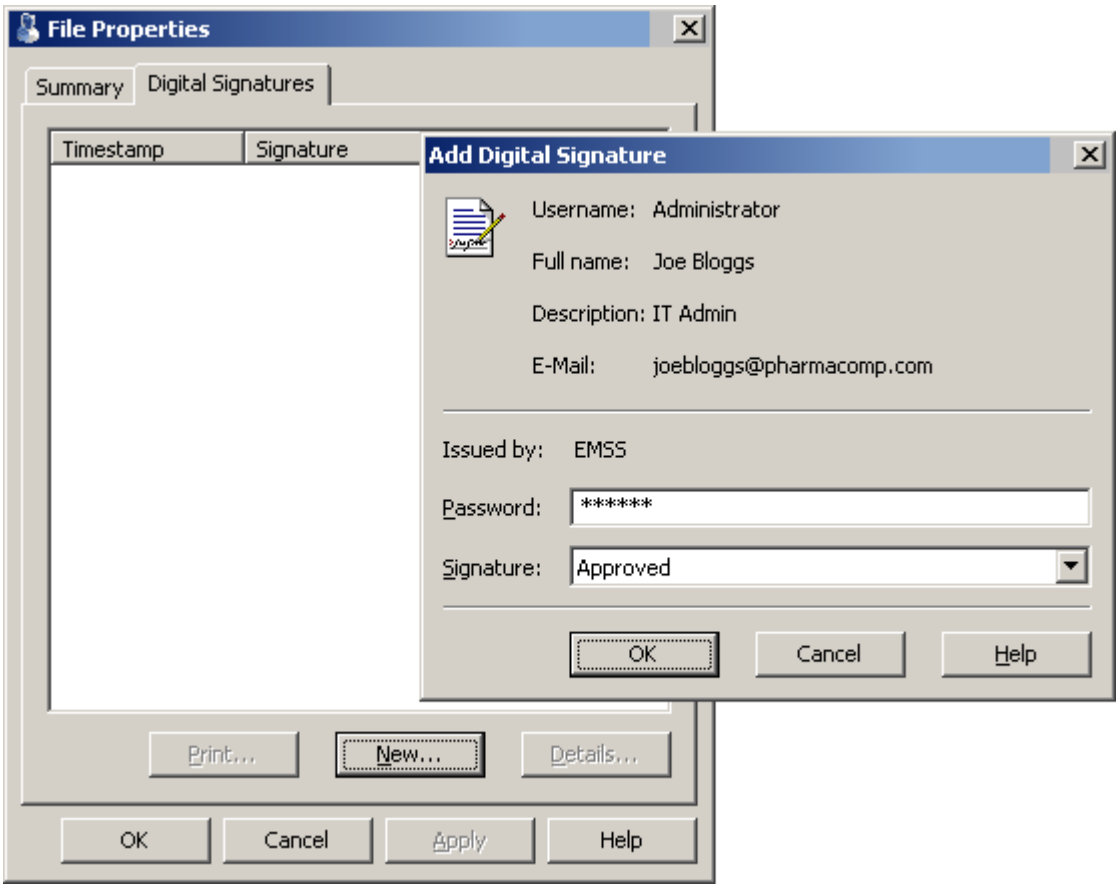
Click on **FILE** and select the file to be signed from the menu.

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



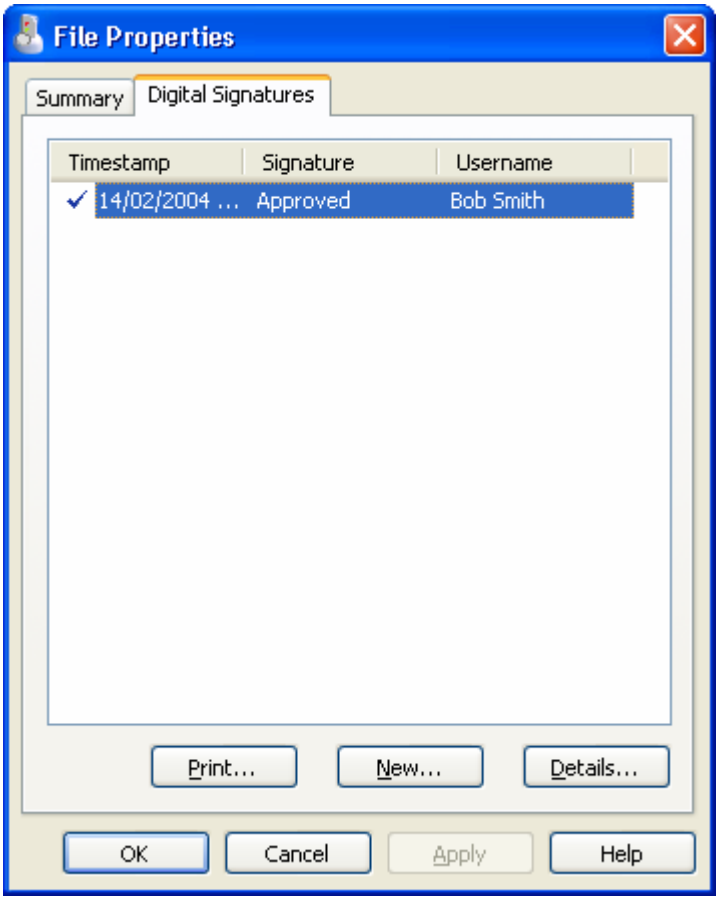
Enter the user's password.

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 multiple 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.

LogTag® Event Viewer

LogTag® Event Viewer is a tool that allows display of the events generated by LogTag User Server.

The software is normally installed and run on the same computer that is running LogTag 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 generated by LogTag User Server.

The Event Viewer software will only display the contents of the audit event log files, but is not permitted to make any modifications to the files. The event logs are stored in files with date coded unique file names either daily, weekly, monthly or yearly at a file location as defined in the LogTag User Server configuration.

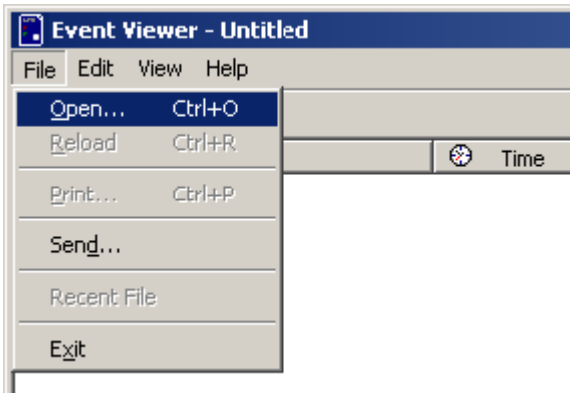
To start LogTag®Event viewer either double click the desktop icon or run from the Programs list off the start menu.

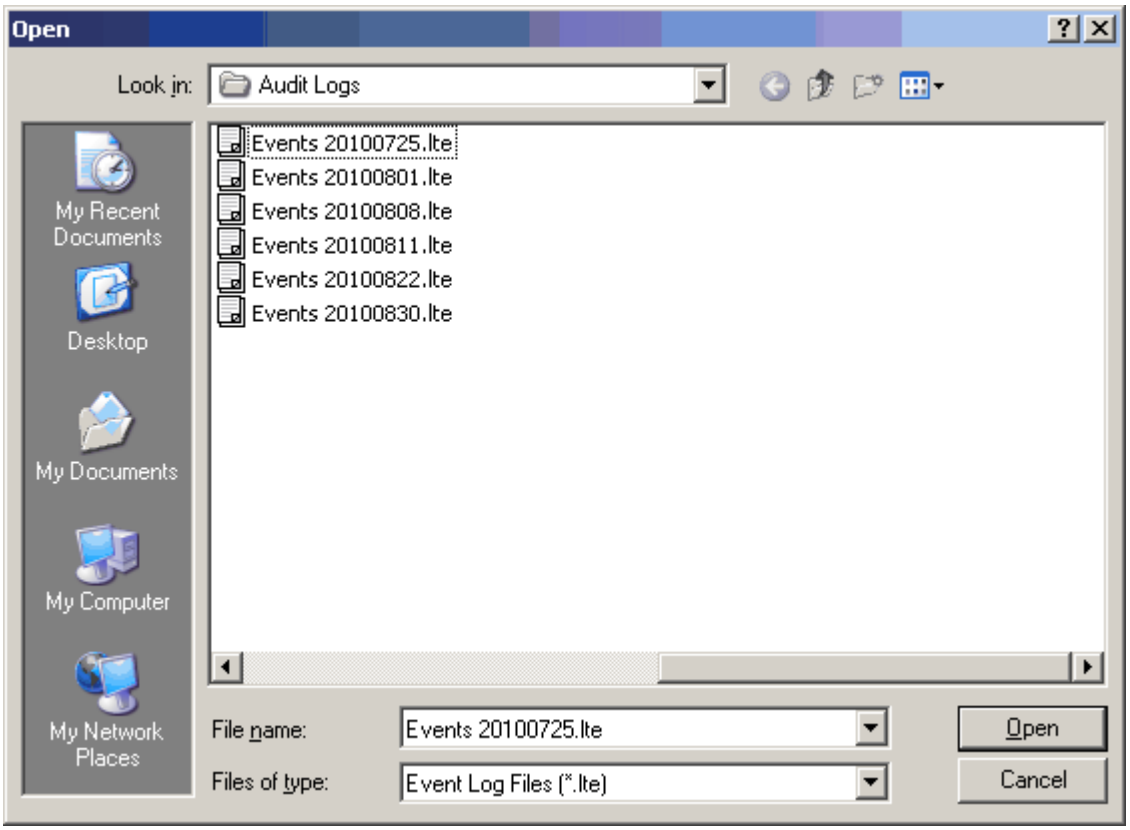
Opening an Event Log File

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 the LogTag User Server configuration.

If the Event viewer is running on a different computer to the one running LogTag User Server then the drive and directory on the computer where the event log files are being stored need to be shared out to the network, preferably with only 'Read only' access.



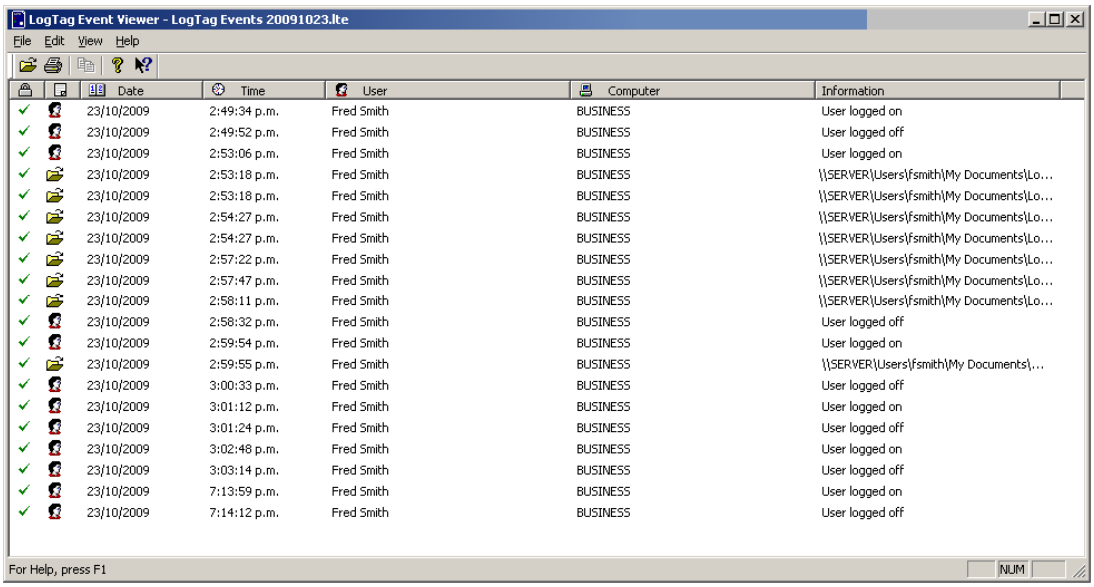


Double click on the file to open or select and click **OPEN.**

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:

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

Table 1: Event Viewer Column definitions

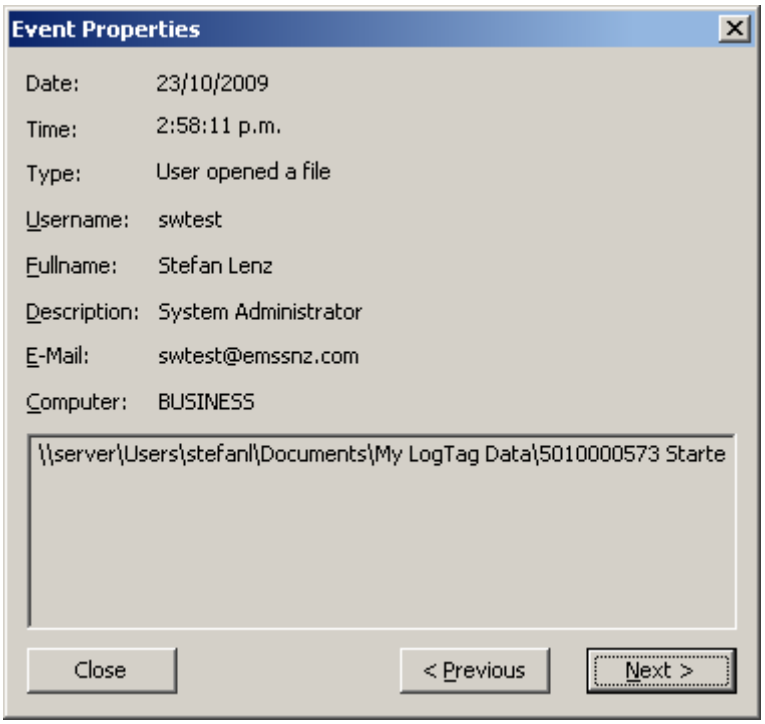
If desired, click on a specific column heading to sort the list by that content.

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

Table 2: Event Viewer Event Symbol definitions

Examining the Event Content

Double click on any event to examine its contents 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.