



## Digital Signatures

### User Guide

### User Server & Event Viewer

Document Release Version: 2

Published July 15, 2022

Copyright © 2004-2022, LogTag North America

## Table of Contents

Copyright .....	3
Disclaimer .....	3
Introduction .....	4
System Requirements .....	6
Installation Considerations .....	7
Networked Installations .....	7
Stand-Alone Installations .....	7
System Installation .....	8
Step 1 – Install User Server .....	8
Step 2: Install the Event Viewer software .....	8
Step 3: Install LogTag® Analyzer software .....	9
Updating .....	9
Configuring LogTag® User Server .....	10
Initial Set-up .....	10
Enabling the Administrator Account .....	14
Editing Settings .....	15
Enter Signature information .....	17
Entering User Information .....	18
Assigning Signatures to Users .....	19
User Permissions .....	20
Configuring Audit Events .....	21
Failure Events .....	22
Successful Events .....	22
Audit Log Settings .....	23
Stopping LogTag® User Server .....	24
Configuring LogTag® Analyzer .....	25
Adding a Digital Signature to a LogTag® file .....	27
Viewing Digital Signatures .....	29
LogTag® Event Viewer .....	30
Opening an Event Log File .....	31
Viewing the event list .....	32
Examining the Event Content .....	34
Appendix A: Installing and Running User Server as a Service .....	35
Appendix B : FDA 21 CFR Part 11 introduction .....	38

## Copyright

The information contained in this document regarding LogTag® User Server software usage is intended as a guide and does not constitute a declaration of performance. The information contained in this document is subject to change without notice. Unless otherwise noted, the example companies, organizations, email addresses and people depicted herein are fictitious, and no association with any real company, organization, e-mail address or person is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

No representation or warranty is given and no liability is assumed by LogTag North America 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.

Copyright © 2004–2022 LogTag North America. All rights reserved.

LOGTAG is a registered trademark (®) of LogTag North America.

## Disclaimer

LogTag User Server is a utility that allows system administrators to deploy a user login system for LogTag® Temperature and Humidity loggers, 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 North America limits the release of this utility 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 1.3r2 or later
- LogTag® Event viewer 1.1 or later
- LogTag® Analyzer 1.3 or later

# Introduction

The Digital Signatures support suite of software has been developed to support the FDA 21 CFR Part 11 standard (see [Appendix B : FDA 21 CFR Part 11 introduction on page 38](#)). 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 North America uses a “client-server” approach for authenticating users and digital signatures.

The client software is LogTag<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> Analyzer, provided security issues are observed.

The LogTag<sup>®</sup> User Server software contains a directory database that authenticates users, grants access to using LogTag<sup>®</sup> Analyzer functions, permits users to digitally sign electronic records created by LogTag<sup>®</sup> Analyzer and maintains the audit event log of user activities.

The Event Viewer is a utility program that allows viewing of the audit logs. It can be run on any computer with access to the location of the event audit log files within the network.

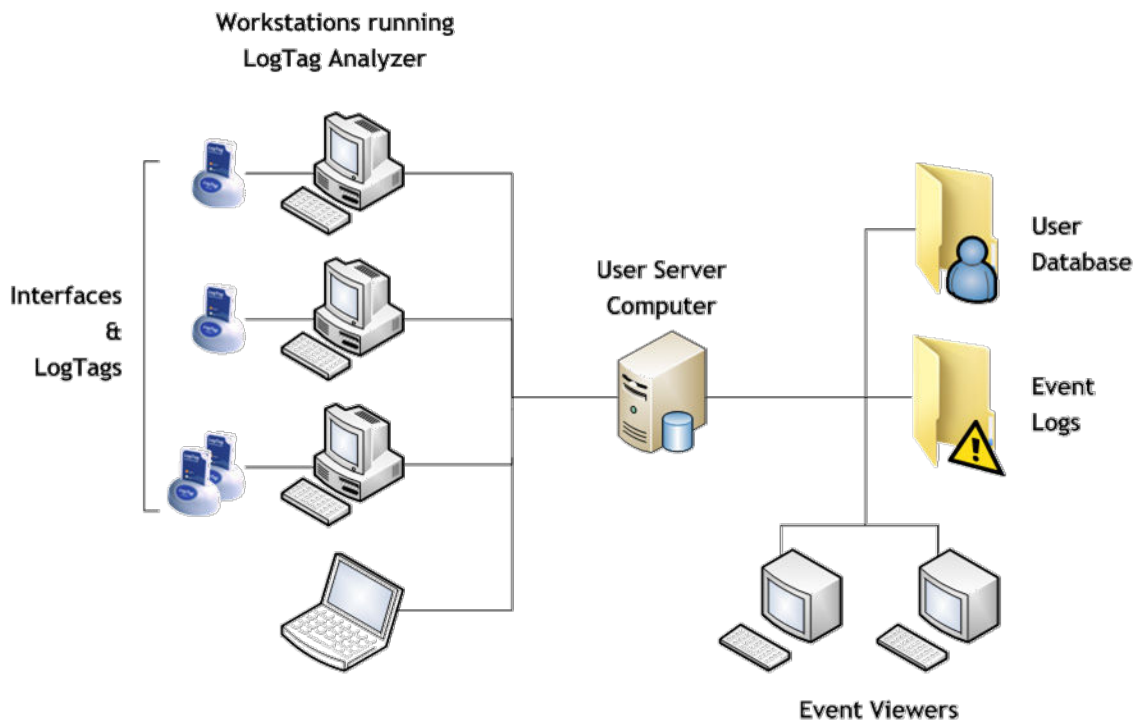


Figure 1: System Diagram

The user server concept allows user/password and event audit management across a LAN or WAN using the TCP/IP network protocol to transfer data (such as users/passwords and events) between a central location and LogTag<sup>®</sup> 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 7 or later, or Windows 2008 Server R2 or later
- 35MB of free disk space
- 1024 x 768, or higher, screen resolution.
- 256 screen colors
- Network card and network access

## Installation Considerations

Software deployment depends on the network structure on the installation site, and the intended audience.

### 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 infrastructure, the LogTag® User Server can be installed on that computer also. It is strongly recommended the administrator password function is enabled in LogTag® User Server to protect the integrity of the system and to prevent unauthorized tampering (see [Configuring LogTag® User Server on page 10](#)).

LogTag North America recommends the use of a central server computer for User Server over running it on a workstation.



## System Installation



You must be logged in with local administrator rights to install the software.

The system consists of 3 applications, which are installed individually.

### Step 1 - Install User Server

LogTag® User Server is the management application for setting up users, signatures and permissions. This application is installed on only one computer.

- Select the computer/server on which to run LogTag® User Server.
- Install the LogTag® User Server software by executing the downloaded file, which will be named `ltserver_13r2.exe` or similar.
- Perform the initial set-up as described in Initial Set-up on page [Configuring LogTag® User Server](#).
- Configure LogTag® User Server as detailed in [Configuring LogTag® User Server on page 10](#).

### Step 2: Install the Event Viewer software

Event Viewer is the application used to view the event logs generated by LogTag® User Server as a result of users interacting with LogTag® Analyzer instances. This application can be installed on multiple computers, but is typically only installed on the same computer that runs LogTag® User Server.

- Select the computers/workstations that will require Event Viewer, and install it by executing the second downloaded file, which will be named `lt_eventViewer_11r1.exe` or similar.
- If you install Event Viewer on a workstation different to LogTag® User Server, you must make sure the event log location on the LogTag® User Server computer is shared with the appropriate permissions (see [Configuring LogTag® User Server on page 10](#)).



### Step 3: Install LogTag® Analyzer software

LogTag® Analyzer is the application used to configure, download, analyze and share data from LogTag® data loggers.

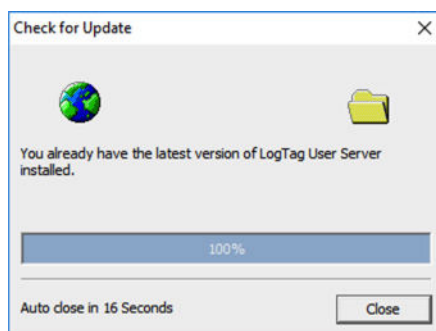
- Install LogTag® Analyzer on as many workstations as required. You can also perform a network installation.
- Setup LogTag® Analyzer according to requirements and the LogTag® Analyzer User Guide.
- Setup LogTag® Analyzer for connection to LogTag® User Server.

### Updating

To update your LogTag® User Server installation, please click **Check Internet for update...** from the **Help** menu. The software will check if a new version is available, and offer a download.

Update the software by executing the downloaded installer file.

You will get a message if no new update is available.



# Configuring LogTag® User Server

To start LogTag® User Server, double-click its desktop icon, or start from the Start Menu.

Once started, LogTag® User Server runs as a background task. You will see the icon in the notification area, however, until the initial set-up is completed, the software is inactive, as shown on the icon.

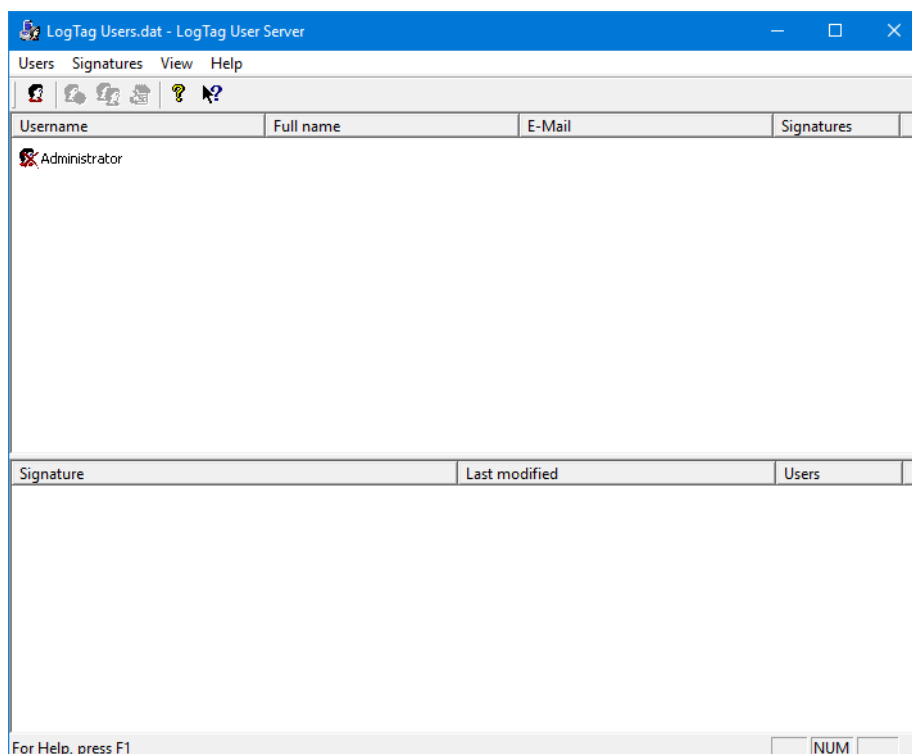


## Initial Set-up

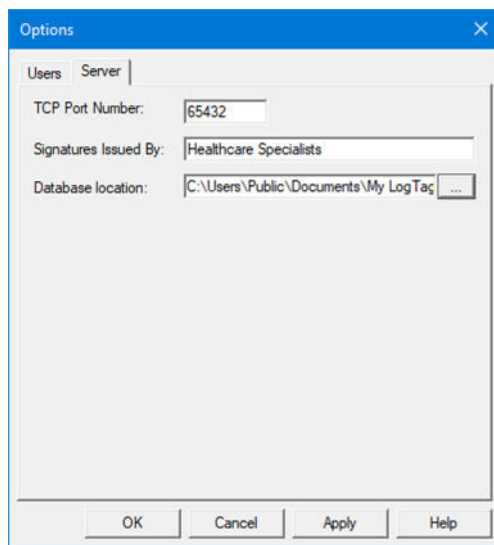
To complete the initial set-up, you must enter basic configuration and connection data:

- Double click the icon in the notification area to open LogTag® User Server, or right-click the icon and click **Restore**.

You will see the main screen.



- Click **Options** from the **View** menu, then click the **Server** tab:



Set following parameters:

- **TCP port number**

Choose a TCP port for connection to the network. 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. Use one of the ephemeral ports, and watch out for ports the system reserves arbitrarily for applications such as Exchange. System administrator can select a port number that best suits the IT system.



Firewalls in the network will need to be configured to allow incoming connections on this TCP port number.

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 organization.

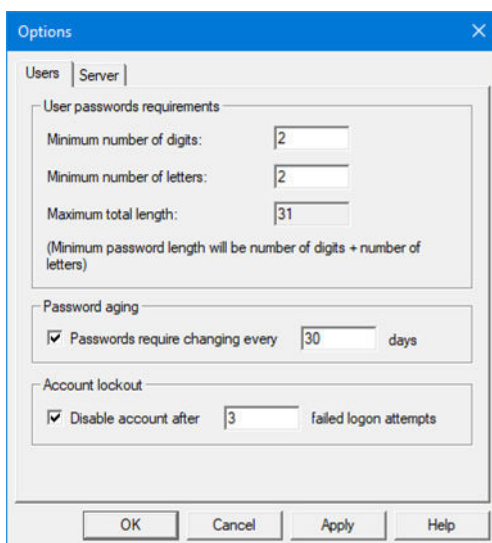
- **Database location**

This is 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.

- **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.

- Click the Users tab

The image shows a screenshot of the 'Options' dialog box with the 'Users' tab selected. The dialog has a blue title bar with the text 'Options' and a close button. Below the title bar, there are two tabs: 'Users' and 'Server'. The 'Users' tab is active. The main area of the dialog is divided into three sections: 'User passwords requirements', 'Password aging', and 'Account lockout'. In the 'User passwords requirements' section, there are three input fields: 'Minimum number of digits' with a value of 2, 'Minimum number of letters' with a value of 2, and 'Maximum total length' with a value of 31. Below these fields is a note: '(Minimum password length will be number of digits + number of letters)'. In the 'Password aging' section, there is a checkbox labeled 'Passwords require changing every' which is checked, followed by an input field with the value 30 and the text 'days'. In the 'Account lockout' section, there is a checkbox labeled 'Disable account after' which is checked, followed by an input field with the value 3 and the text 'failed logon attempts'. At the bottom of the dialog, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Amend the following parameters, or leave them at their default value:

- **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 behavior 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.

Once configured, LogTag® User Server will become active, as shown in the icon in the notification area. If at any time you wish to make changes to any of the data, you must enter the administrator user name & password, which is not required on first time configuration, or until you have activated the administrator account.

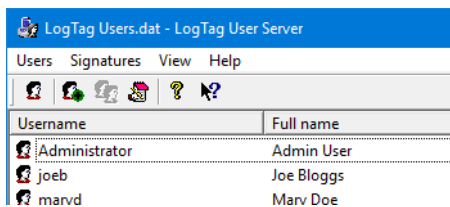


## Enabling the Administrator Account

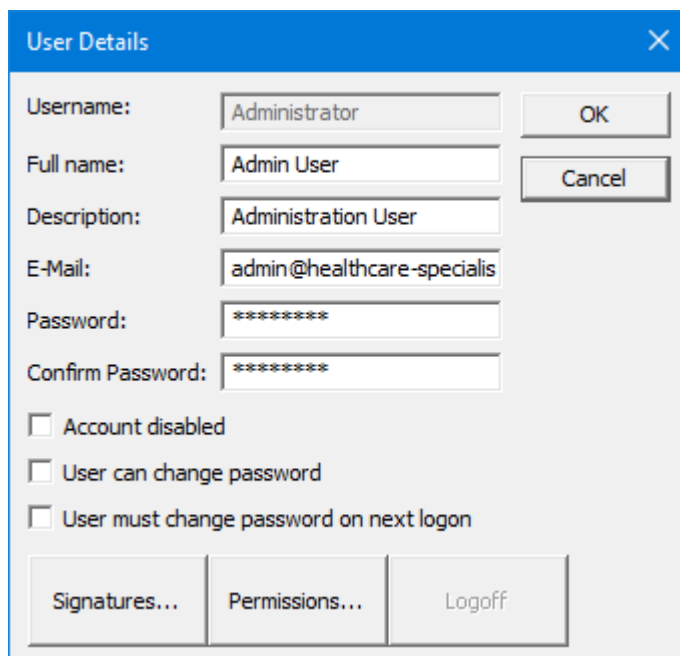
If you want to secure your installation against unauthorized use, you need to enable the Administrator account. If you do not enable this account, anyone with access to the computer can make changes to the entire LogTag® User Server database. Therefore, we highly recommend you enable this account.

Once enabled, the administrator user is the only user with the ability to manage the server database and configuration, and to make any changes, the administrator must be logged on with the administrator credentials.

To configure the administrator password, double click the administrator user or click **Edit...** from the **Users** menu.



The User Detail screen for the Administrator is displayed:

The screenshot shows the 'User Details' dialog box for the 'Administrator' user. It contains the following fields and options:

- Username: Administrator
- Full name: Admin User
- Description: Administration User
- E-Mail: admin@healthcare-specialis
- Password: (masked with asterisks)
- Confirm Password: (masked with asterisks)
- ☐ Account disabled
- ☐ User can change password
- ☐ User must change password on next logon
- Buttons: OK, Cancel, Signatures..., Permissions..., Logoff

- Enter the administrator's details and a password.

**DO NOT LOSE THIS PASSWORD**

You will not be able to make any changes to your installation if you lose this password, and you are logged off!

LogTag North America will not be able to recover this password for you.

- Enable the account
- Change the password settings as desired
- Click **OK**.

The standard user list is shown.

From this point on, any changes to the LogTag North America database can only be made when logged on with the administrator account (select **Logon** from the **Users** menu). Once you have made any required changes, log off (select **Logoff** from the **Users** menu).

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. The installation is now open again for everyone to edit.

## Editing Settings

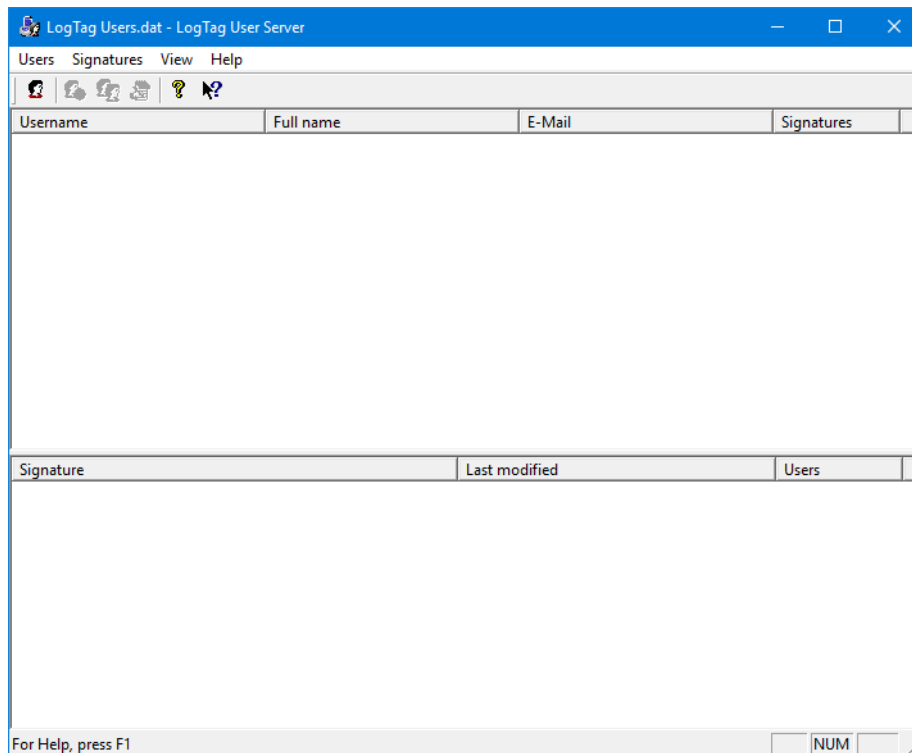
Double click the User Server icon in the notification area to open the user server main window. If you cannot see the icon, it may be hidden, so you need to **Show hidden items** on the taskbar to access it.



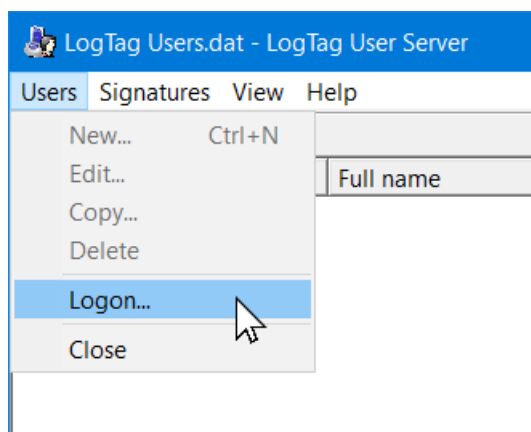
You need to use a special procedure if LogTag® User Server is installed as a service. Please see [Appendix A: Installing and Running User Server as a Service on page 35](#)



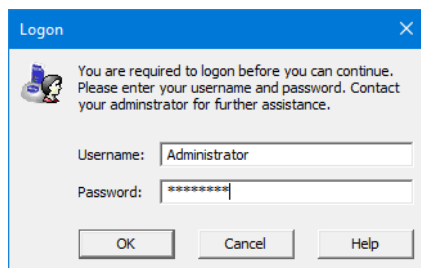
If you have activated the administrator account, which means user server is password protected, blank entries are displayed and you will need to log on as the administrator to gain access.



Click **Logon** from the **Users** menu.

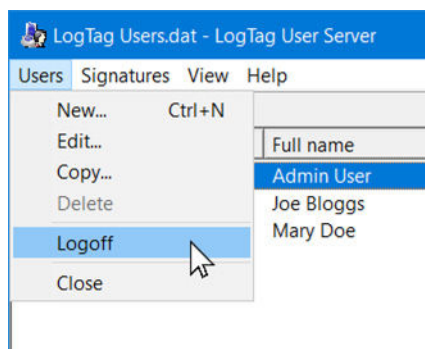



Enter the username and password for the just configured administrator account.



After a successful login, the user server window will display the current user database settings and the associated menus will become accessible.

Once you have completed your tasks with LogTag® User Server, logoff the Administrator account by selecting **Logoff** from the **Users** menu.



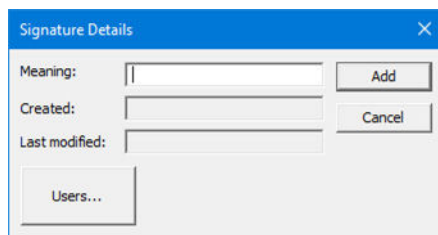
Once logged off the blank user server screen will re-appear. Click  to close the window.

## Enter Signature information

An electronic signature is a piece of unique digital information contained in a file, that can be attributed to a specific user. Each signature has a special meaning, and is usually used to record decisions made relating to the data it contains.

For users of LogTag® Analyzer to add signatures to files, these have to be added and their meaning defined. This is done in the Signature Details window.

- Click **New...** from the **Signatures** menu.

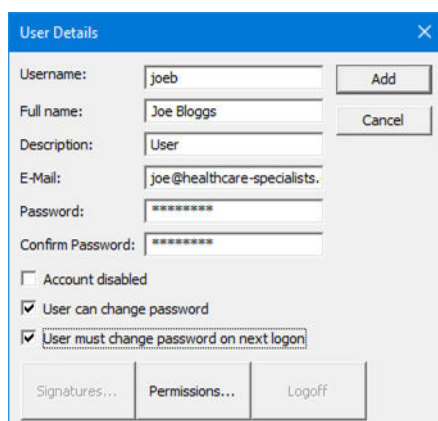
A dialog box titled "Signature Details" with a close button (X) in the top right corner. It contains three text input fields: "Meaning:" with a value of "I", "Created:" which is empty, and "Last modified:" which is empty. To the right of the "Meaning:" field is an "Add" button, and to the right of the "Created:" field is a "Cancel" button. At the bottom left is a button labeled "Users...".

- Enter the meaning of the signature, for example, "Approved", "Rejected", "Quarantine".
- Click **Users** to add or remove users' permission to use 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 **Edit...** from the **Signatures** menu.

## Entering User Information

Each user must have a valid logon and password to perform any action in LogTag® Analyzer. This information is entered in the User Details window:

- Click **New...** from the **Users** menu.

A dialog box titled "User Details" with a close button (X) in the top right corner. It contains several text input fields: "Username:" with a value of "joeb", "Full name:" with a value of "Joe Bloggs", "Description:" with a value of "User", "E-Mail:" with a value of "joe@healthcare-specialists.", "Password:" with masked characters "\*\*\*\*\*", and "Confirm Password:" with masked characters "\*\*\*\*\*". To the right of the "Username:" field is an "Add" button, and to the right of the "Full name:" field is a "Cancel" button. Below the input fields are three checkboxes: "Account disabled" (unchecked), "User can change password" (checked), and "User must change password on next logon" (checked). At the bottom are three buttons: "Signatures...", "Permissions...", and "Logoff".

- Enter the user information and password as prompted.
- Enable the options as appropriate for the user concerned.

- The **Permissions** button allows configuration of what actions and resources a particular user has access to (see [User Permissions on the next page](#)).
- The **Signatures** button allows association of existing signatures types to this user (see [Assigning Signatures to Users below](#)).
- Click **Add** to add this user.

The user name will appear on the main screen. When you have finished adding users, click **Close**.

A user's information can be modified by highlighting the user name in the main window and clicking **Edit** from the **Users** menu.



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 where a valid Windows logon has been provided.

## Assigning Signatures to Users

You can add which signatures a user can apply when you set up the user, or afterward by editing the user information (highlight the user name and clicking **Edit** from the **Users** menu).

User Details

Username: joeb OK

Full name: Joe Bloggs Cancel

Description: User

E-Mail: joe@healthcare-specialists.

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

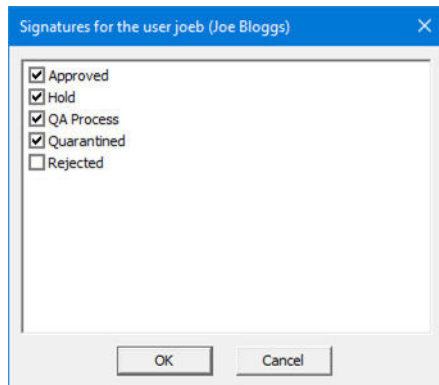
☐ Account disabled

☒ User can change password

☒ User must change password on next logon

Signatures... Permissions... Logoff

- From the **User Details** screen, click **Signatures...** to show the signatures currently allocated to the user.



- Enable each signature you want this user to be authorized to apply.
- Click on OK to save the changes.

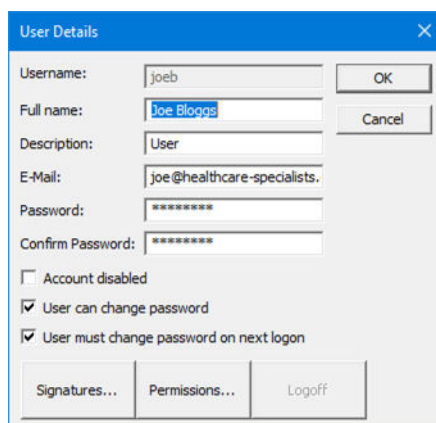
For example, the user **joeb** cannot reject a shipment, as he is unable to apply the "Rejected" signature.

The number of signatures for which that user is authorized will appear on the main screen against the user name.

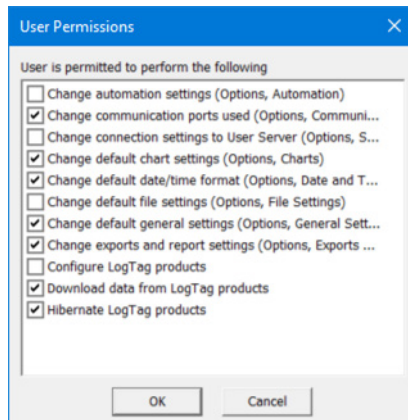
## User Permissions

Once LogTag® Analyzer is connected to LogTag® User Server, you can restrict what users can do once they are logged on.

You can set permissions for a user when you set up the user, or afterward by editing the user information (highlight the user name and clicking **Edit** from the **Users** menu).



- From the **User Details** screen, click **Permissions...** to show the permissions that can be enabled or disabled.



- Enable or disable permissions as desired. The screen above shows a typical permission set for a user who is allowed to download logger, but cannot change storage settings. By default, all permissions are enabled.
- Ensure that users cannot change User Server settings, as this would enable them to disconnect LogTag® Analyzer from the User Server installation.

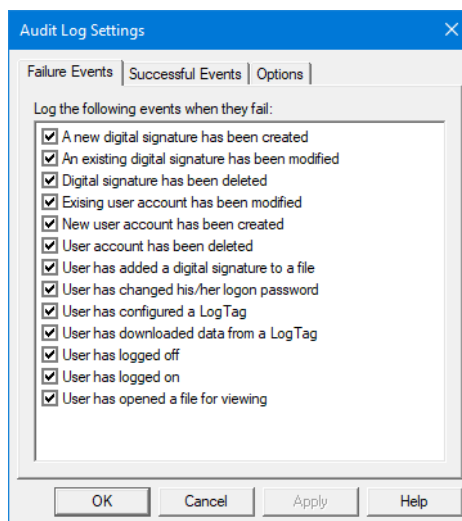
Click **OK** to save the permissions.

## Configuring Audit Events

Audit Events track each user's actions as a time & date stamped events which are stored in an event file (see page [LogTag® Event Viewer](#)). The actions to be logged and the event log files location can be configured by accessing the Audit Events settings.

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

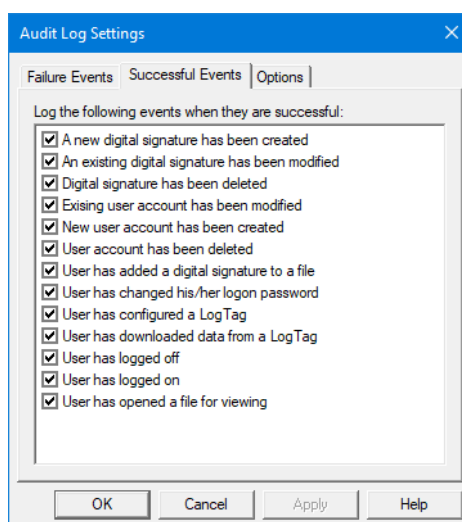
## Failure Events



The list shows possible actions that may fail (such as a user was unable to configure a logger).

Set a tick box for each event where you wish to record in the event audit log if a failure occurs. Clear the tick for each action that you do not want to record. By default, all actions are enabled for recording.

## Successful Events



Click the **Successful Events** tab.

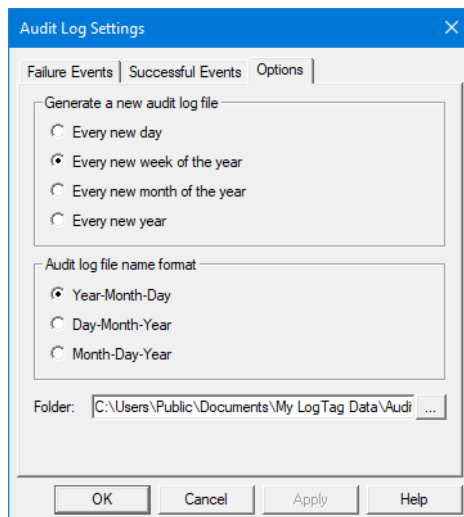
You see a list with the same entries. Enable or disable which successful events will be recorded. Again, all events are enabled by default.



## Audit Log Settings

Click 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. You can also determine the make up of the file name generated for this period.



The Folder entry defines the location of the event audit files – this location can be changed to suit the installation site requirements. Users who want to access the event logs with Event Viewer will need to know this location. If the Event Viewer is used on a different computer, this location needs to be shared with at least read permission.

Click  to view or change the Audit Events folder location.

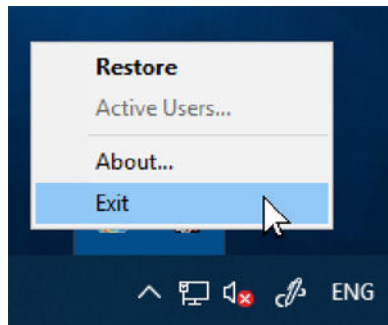
The default location for Windows 7 or newer operating system is:

**C:\Users\Public\Documents\My LogTag Data\Audit Logs**

The Event Viewer software will not delete any audit log files (no rotation policy), so it is up to the administrator to ensure there is enough disk space available for the audit log files.

## Stopping LogTag® User Server

To stop LogTag® User Server, right-click the icon in the notification area and click **Exit**.



It is not sufficient to close the application window to stop LogTag® User Server.

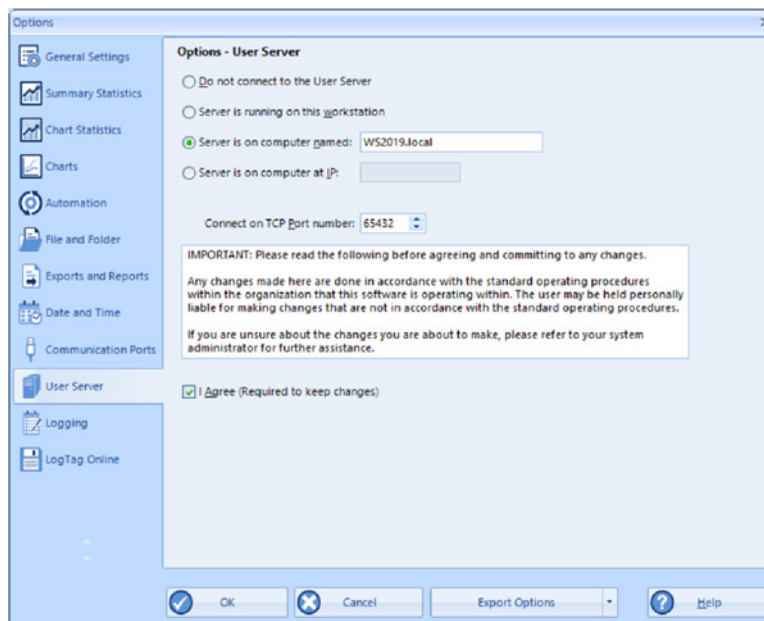
Please note that -once stopped- users with LogTag® Analyzer installations connected to this instance of LogTag® User Server will no longer be able to use LogTag® Analyzer until LogTag® User Server is restarted.

## Configuring LogTag® Analyzer

To make use of the features that LogTag® User Server provides, LogTag® Analyzer must be connected to LogTag® User Server.

Start LogTag® Analyzer and click **Options** from the **Edit** menu.

Select the **User Server** tab.



Choose the option that matches the set up of your network:

- Select **Server is running on this workstation** if LogTag® User Server and LogTag® Analyzer are running on the same workstation.
- Select **Server is on a computer named** if LogTag® User Server is running on a server or another workstation with a known computer name.
- Select **Server is on computer at IP** if LogTag® User Server is running on a server or another workstation with a fixed and known IP address.

Enter the TCP port number as configured in LogTag® User Server.

Read the notice and click **I Agree**. A connection test will now determine if the User Server instance can be reached. Only if this test is successful, a tick will appear, and only then will you be able to click OK to close the dialog and activate the new settings.

If you receive an error message that LogTag® User Server cannot be reached, we suggest to use a tool such as `portqry` to check the port on the target PC can be reached.

```
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>portqry -n WS2019.local -e 65432

Querying target system called:
    WS2019.local

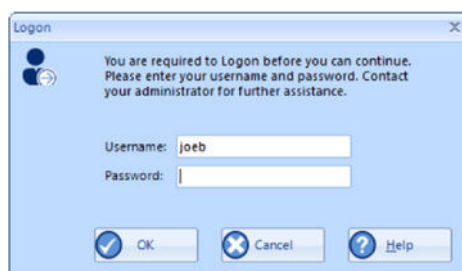
Attempting to resolve name to IP address ...

Name resolved to 192.168.100.105

querying ...

TCP port 65432 (unknown service): LISTENING
```

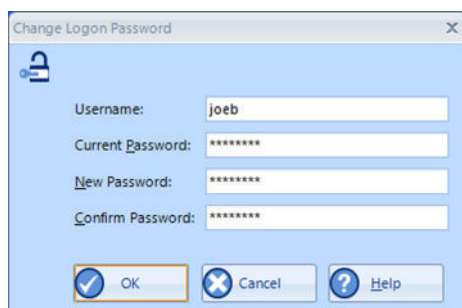
A user with an active account must now log on to continue using LogTag® Analyzer. The logon dialogue will be displayed:



Enter a valid username and password to continue.

When you first log on, or at any time the administrator is requesting it, you are asked to change the password for accessing LogTag® User Server.

Following window will be shown:



Enter your old password, your new password and confirm it. Click OK to save the new password. If LogTag® User Server has requested a password change,

LogTag® Analyzer will not let you continue until you have confirmed the change.



LogTag® User Server does not enforce unique passwords, so you can re-use your old password if you desire. Note, however, that this is not good practice.

## Adding a Digital Signature to a LogTag® file

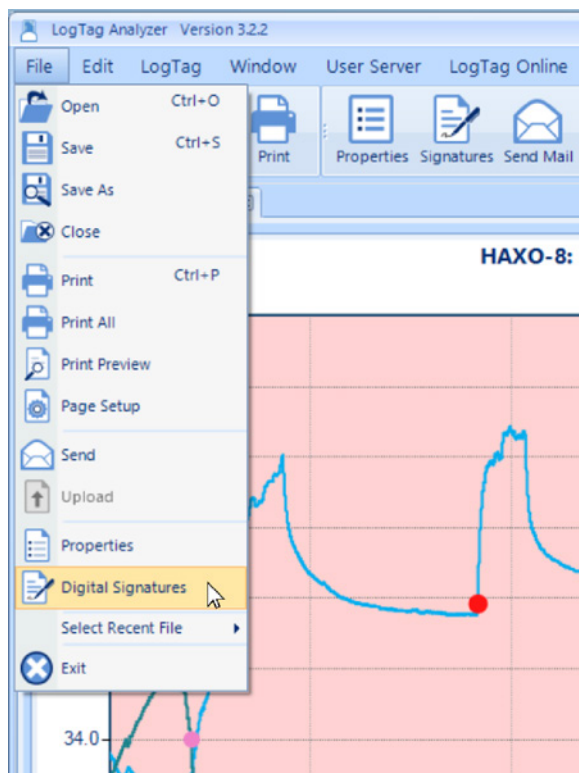
To add digital signatures to files:

- 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.
- A user must be successfully logged on to LogTag® Analyzer.
- The user must have been authorized to add digital signatures.

Start LogTag® Analyzer and log on with your user name and password.

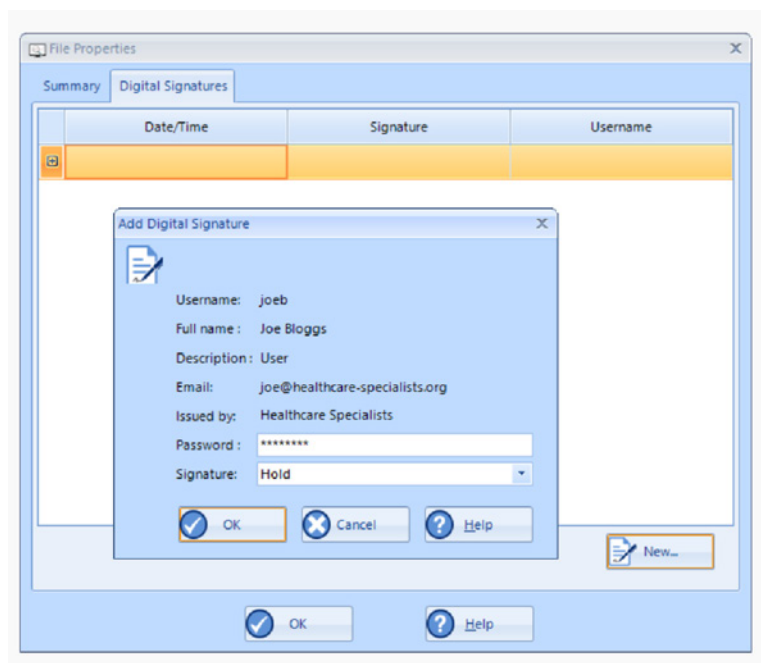
The standard LogTag® Analyzer screen will be displayed, with the menus accessible according to the user's permission settings.

Open any file to be signed. Click **Digital Signature** from the file menu or **Signatures** from the toolbar.



The **File Properties** window will be displayed, with the **Digital Signatures** already active.

- Click **New**. The **Add Digital Signature** window is shown.



- Enter your password.

- Select the signature required from your list of authorized signatures and click **OK**.
- Repeat the process if you need to add additional signatures (each file is capable of storing multiple digital signatures).

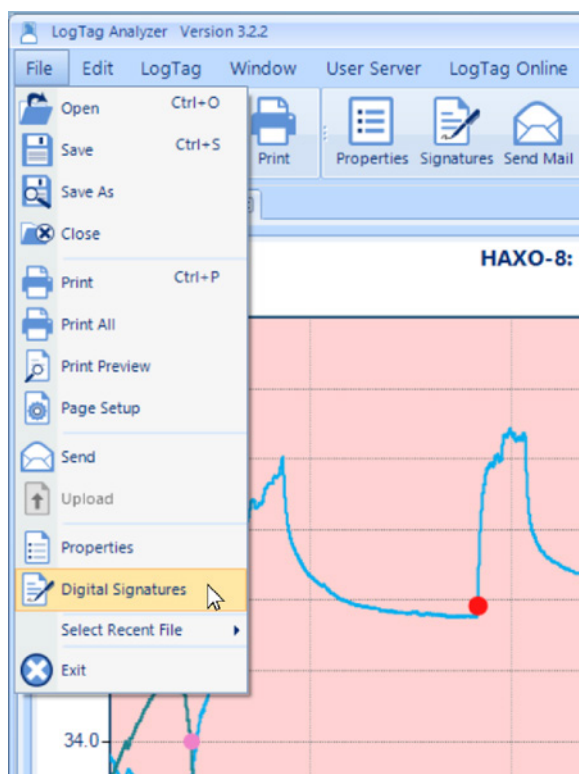
Click **OK** to close the **File Properties** window.

## Viewing Digital Signatures

Start LogTag® Analyzer and log on with your user name and password.

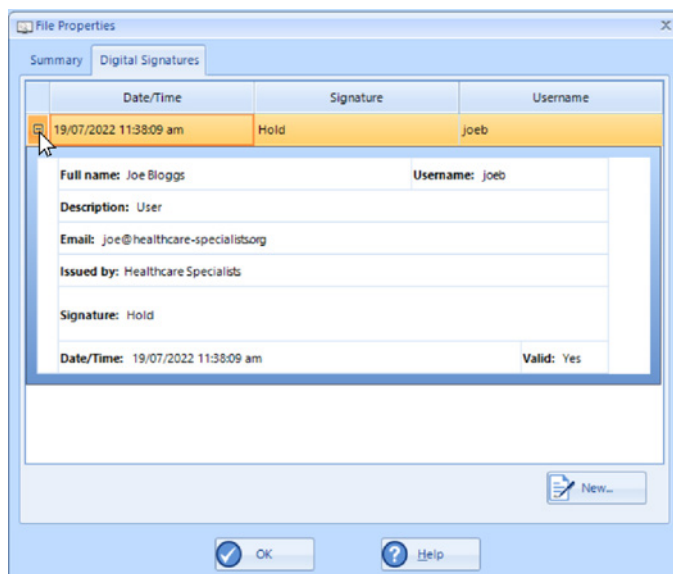
The standard LogTag® Analyzer screen will be displayed, with the menus accessible according to the user's permission settings.

Open any signed files. Click **Digital Signature** from the file menu or **Signatures** from the toolbar.



The **File Properties** window will be displayed, with the **Digital Signatures** already active. It shows the list of the digital signatures currently included in the file. These signatures are permanently included in the file and cannot be removed. Click the plus icon on the left to show the signature's details:





The Events Info section of the report (accessible via the Report tab) shows that a digital signature was applied to the file.

#### Events Info

15/12/2010 5:52:30 pm	Download
16/12/2010 7:28:00 am	Inspection
19/07/2022 11:38:09 am	Digital Signature applied Signature: "Hold", Username "joeb"

Source: HAXO-8\_Testfile\_1.ltd

## LogTag® Event Viewer

Each event captured by LogTag® User Server generates an entry in an event log file. A new event log file is generated as soon as the first event is recorded, and subsequently at a frequency defined in LogTag® User Server (see [Configuring Audit Events on page 21](#)).

The files contain the creation date as part of their name, in the format you define in the LogTag® User Server settings, for example LogTag Events `yyyymmdd.lte`.

LogTag® Event Viewer is a tool that allows displaying of the event log files generated by LogTag® User Server .

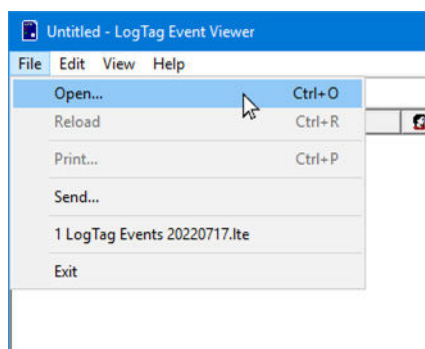
Event Viewer is normally installed and run on the same computer that is running LogTag® User Server, however, it can be operated on any computer,

provided it can gain access to the folder that contains the audit event log files generated by LogTag® User Server.

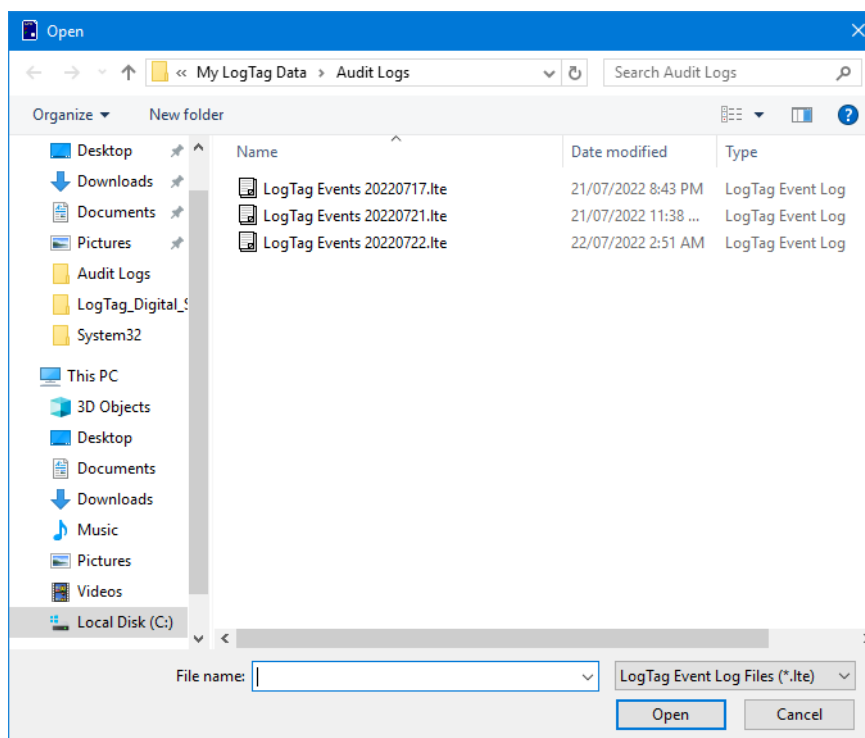
The Event Viewer software will display the contents of the audit event log files, but is not permitted to make any modifications to the files.

## Opening an Event Log File

To view the events from a log file, open the log by clicking **Open** from the **File** menu, or by clicking **Open** from the toolbar.



You will see the default location with the event files recorded to date. If the Event viewer is running on a different computer to the one running LogTag User Server, browse to the defined network location.



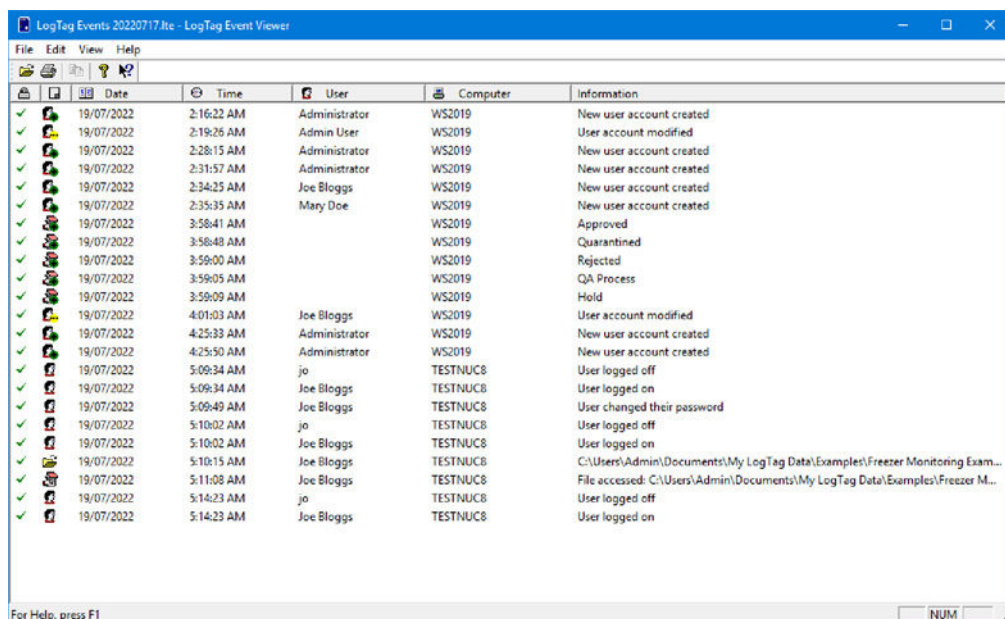
Double click a file to open it or select and click **Open**.

You can also directly select a file from the recently opened files list.

## Viewing the event list


Event records from an opened file are displayed as a 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 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 (see following table for more information)
Date	Date the event occurred
Time	Time the event occurred
User	The name of the user that generated the event

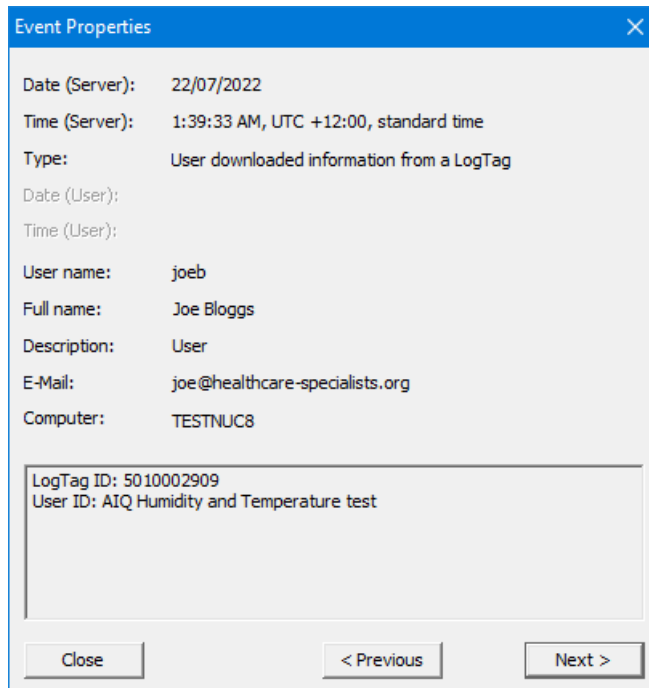
Column	Content
 Computer	The name of the computer the event was generated on
Information	Summary information about the event

If desired, click a specific column heading to sort the list by that content in ascending or descending order.

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

## Examining the Event Content

Double click any event to examine its contents.



Click **Next** or **Previous** to navigate through the list, or **Close** to close the Event Properties window.

## Appendix A: Installing and Running User Server as a Service

If LogTag® 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 LogTag® User Server as a service with the help of the Windows Server 2003 Resource Toolkit. This procedure needs to be performed after User Server has been installed on the network server computer.



This technique is directed towards experienced network professionals who are familiar with the procedures required and the risks involved. It requires 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 North America will only provide very limited support.



This procedure has been written for and been tested with Windows Server 2019 Essentials. Although the Windows Server 2003 toolkit still works with even the latest Windows Server operating systems, support for the toolkit has ended with Windows Server 2003. An open-source project `srvany-ng` is available at [github](https://github.com/birkett/srvany-ng) (<https://github.com/birkett/srvany-ng>) which introduces 64-bit compatibility. Neither of these tools are provided by LogTag, and you use them at your own risk. Some limited support documentation is available from the Microsoft Knowledge Base at <https://docs.microsoft.com/en-US/troubleshoot/windows-client/deployment/create-user-defined-service>.



The tools necessary to perform this procedure are no longer provided with any server OS, they are, however, still available for download.

Please consult the Microsoft Knowledge Base for further information regarding your specific OS.

1. Install the Windows Resource Tool kit for your operating system. Note the installation path to the "tools" folder. Some older 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 an elevated command prompt.
3. Type `"PATH_TO_TOOLKIT\INSTSRV.EXE" LTUserServer "PATH_TO_TOOLKIT\SRVANY.EXE"` where `PATH_TO_TOOLKIT` is the drive and directory of the Windows Resource Kit, for example `"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<sup>®</sup> User Server executable, for example "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.



The User Server service is now owned by the SYSTEM account. If you wish to change any settings in User Server, it is not sufficient to just open the program from the notification area. Instead, you need to do the following:

1. Stop the service from the Services console.
2. Start User Server by double clicking on the desktop icon or through the Apps shortcut.
3. Log on and make the desired changes.
4. Close the User Server program and exit the program from the notification area in the taskbar.
5. Start the service from the Services console.

## Appendix B : 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.