Feature Database Manager

LabSpeed User Management and Security

Topos Technologies, Inc.

Table of Contents

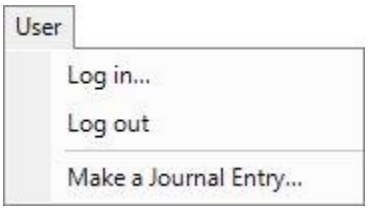
Feature Database Manager Overview

Feature Database Manager is a LabSpeed Feature add-in that provides SQL Server database support for the following LabSpeed security options

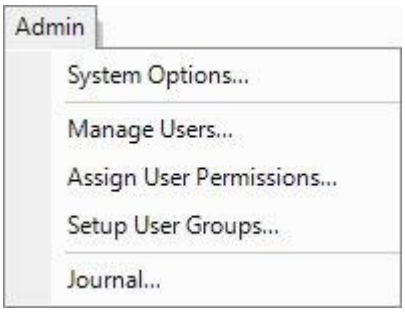
- User Management using Windows login credentials for verification
- Permission Groups for *Administrator*, *Power User* and *User* user types
- Individualized User Permissions
- 21-CFR Part 11 Compliance
- Journal

An Administrator can setup the security environment for LabSpeed to control how users in the lab will interact with LabSpeed and optionally force compliance with 21-CFR Part 11 regulations.

Two new top level LabSpeed menu items are added when the Feature Database Manager is active:



User Menu



Admin Menu

Summary of Security Features

- The *User* menu allows a user to log in and log out. The *Admin* Menu provides access to Options, User and Permission management and the Journal. *System Options* is where an administrator will enable Permissions and 21-CFR Part 11 compliance. By default, they are turned OFF.
- There is a default administrator user. Username = **"Administrator"**, Password = **"Administrator"**. Log on as the default administrator user to access the *Admin* menu items. It may be disabled later once other administrator users are assigned.

- All assigned Users must have active Windows log-in credentials. When a user logs into LabSpeed, his Windows log-in credentials are tested; if they pass, then the user is logged in.
- Users may be assigned a Permission Group -- “Administrator”, “Power User” or “User”. “Administrator” users always have all permissions. You can choose how the “Power User” and “User” groups are setup and what options will be available to each.
- Individual users can be assigned Permissions that are allowed for his/her group. When a new user is added, all permissions are off for that user by default. You will have to turn on some or all permissions for each added user.
- When the 21-CFR P11 Option is turned ON, a User must be 21-CFR Compliant in order to log into LabSpeed. A user is 21-CFR compliant if there is a Full Name associated with his LabSpeed user credentials.
- When a user logs in, actions that are not allowed will be disabled in the toolbar and menus. When no-one is logged in, all permission actions are disabled.
- The Journal tracks changes to Permissions and Options.
- A Special 21-CFR Signature View may be added to any Session/Template (drop down the Special Views toolbar button). Multiple selected samples or experiments may be signed at the same time.
- A report may contain the full name of the logged-in user.
- A journal is maintained to keep track of option and permissions settings and users who log in and log out.
- If a Service is employed to automatically transfer saved data to the Topos SQL Server database, it may be setup to participate in the user permissions and 21-CFR authoring of samples and experiments.

System Options

To access the System Options, you must be logged in as an Administrator. Before any users are added, including administrators, you can log in using the default Administrator user name and password. This user can be used initially until an actual Administrator and password are added and can then be disabled for security.

Default Administrator User Credentials
Username = "Administrator"
Password = "Administrator"

Click on the Admin->System Options menu item. The following dialog is displayed:

Initially, all options are disabled (unchecked). When disabled, LabSpeed runs without users and permissions as if the Feature Database Manager was not installed.

Enabling User Permissions

When User Permissions is enabled, users are required to login in order to use LabSpeed. Any action a user is denied, based on the assigned Permissions for that user, will be disabled in the menus and toolbar.

Enabling 21-CFR Part 11 Compliance

.
When 21-CFR Part 11 compliance is enabled, User Permissions is also enabled and forced on.

When 21-CFR Part 11 compliance is enabled, only users who are 21-CFR P11 compliant may log on and participate in using LabSpeed. Compliance for 21-CFR Part

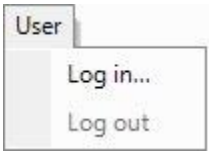
11 is determined by the user's LabSpeed credentials. A user with a valid Full Name (first and last) is considered 21-CFR Part 11 compliant. See Managing Users

Enabling User Lockout after maximum failed log in attempts

When User Permissions is enabled, users are required to login in order to use LabSpeed. The Log in window will automatically exit after a maximum of three (3) failed log in attempts. The Log in window will have to be re-opened to try again. If lockout is enabled and the same user attempted and failed three times to log in, the user will be de-activated. An Administrator is required to re-activate the user. See Managing Users

Logging In / Out

When User Permissions are enabled, a user is required to login to use LabSpeed. To login, go to the *User Menu* and choose *Log In*.



The following dialog is displayed:

Enter your Windows login credentials.

A Maximum of three (3) attempts is allowed before failing to login. You will need to exit and re-enter to try again. If the administrator option is set to lock out the user after three attempts is turned on, the user will be de-activated. An administrator is required to re-activate the user.

Once logged in successfully, the menus and toolbar items are enabled to conform to the user's assigned permissions.

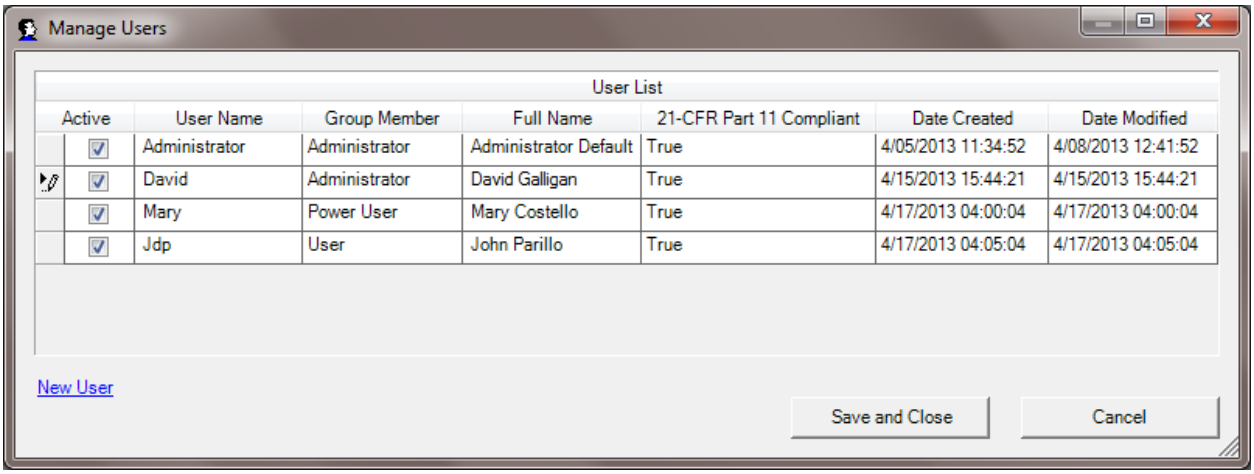
A new user may login without logging out the previous user.

When no one is logged in (at startup and when user logs out), all actions that require a permission are disabled.

Managing Users

To manage users, you must be logged in as an Administrator.

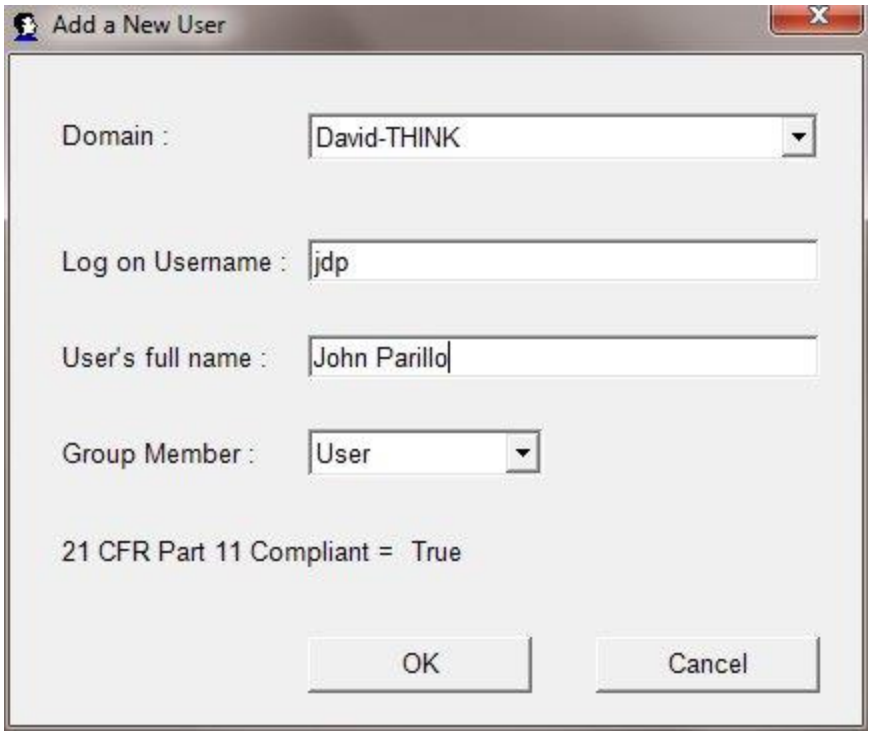
Click on the *Admin->Manage Users* menu item. The following dialog is displayed:



The first entry is the default Administrator. It may be de-activated and activated at any time by an Administrator. Typically, once other Administrators have been added, the default Administrator is de-activated for security, since the password is public.

Creating a New User

Click on *New User* to add a new user to the list. The following dialog is displayed:

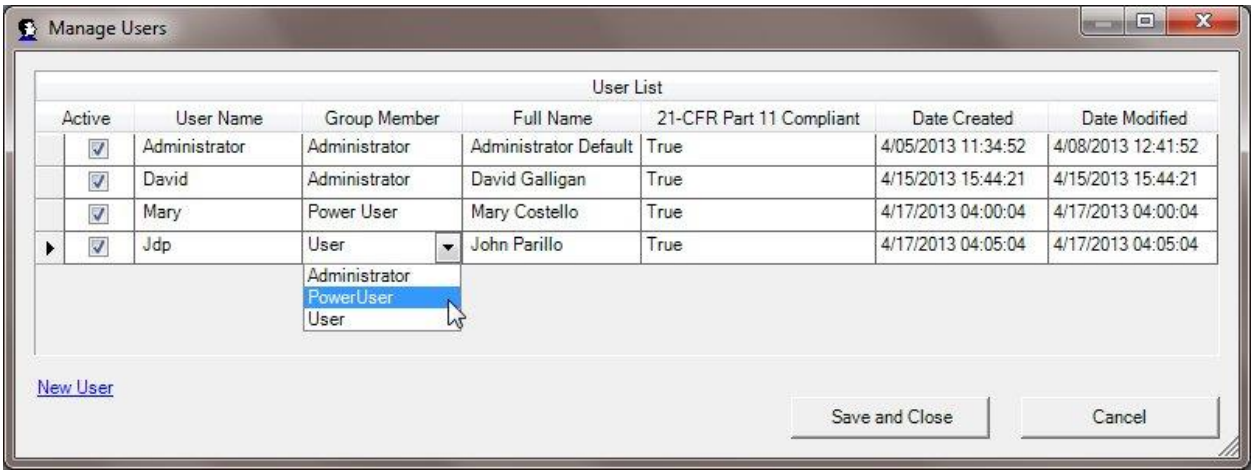


The user's username must be a valid Windows username with Windows user account. In LabSpeed, when someone logs on, the Windows credentials (domain, username and password) are tested. If it passes, then the user will successfully log into LabSpeed. Note that Windows accounts maintain password aging and other criteria important for 21-CFR Part 11 compliance. If a user does not have a Windows account, he/she will not be able to log into LabSpeed.

The user's full name is required for 21-CFR Part 11 compliance. If the user does not have a full name, and 21-CFR P11 compliance is enabled in System Options, then he will not be allowed to log into LabSpeed.

The Group Member is the user's group type -- *Administrator*, *Power User* or *User*. See Permission Groups

Once a new user is added to the list, parts of it may be edited in the table row.



The Group Member, Full Name and Active State may be changed. Note that the User Name may not be changed. To change a user name, that user may only be de-activated and re-added again.

De-activating a User

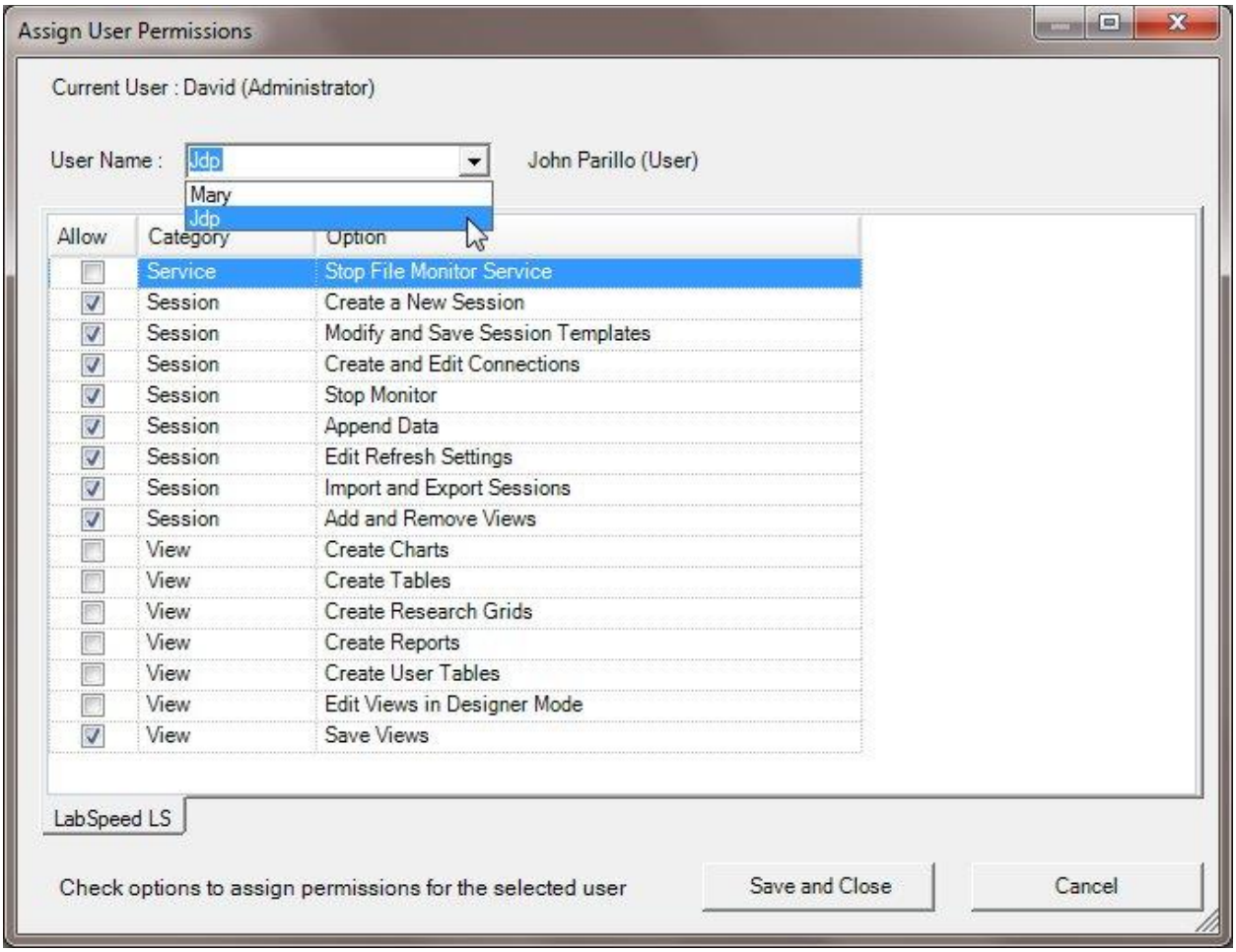
A user may not be deleted. He can only be de-activated, e.g. should a user leave the company or if the user is no longer a valid user. To de-activate a user, un-check the Active state for that user. A user may be re-activated by checking the Active state on.

Assigning User Permissions

To assign permissions to individual users, you must be logged in and have permission. An administrator always has permission.

Every user has been assigned a User Group (*Administrator*, *Power User* and *User*), which defines the range of permissions allowed for each user. An administrator may then customize those permissions for each individual user. For example, one member who is a *Power User* may be allowed to sign samples and another may not.

Click on the *Admin->Assign User Permissions* menu item. The following dialog is displayed:



Select a user to modify in the drop down list. A list of available permissions is presented for that user (this displayed list will depend on the User Group that user is assigned to). Toggle on/off permissions allowed for that user to customize the permission set for that user.

In the example above, the user *Jdp* is assigned simple operating rights and is not allowed to create new Charts, Tables, Research Grids and Reports and not allowed to modify existing ones using the View Designer.

The tab shows the current Application name. Additional tabs may appear depending upon other sources that may require assigned permissions.

Click *Save and Close* to save the changes.

Setting up User Groups

To setup User Groups, you must be logged in and have permission. An administrator always has permission.

There are 3 types of users

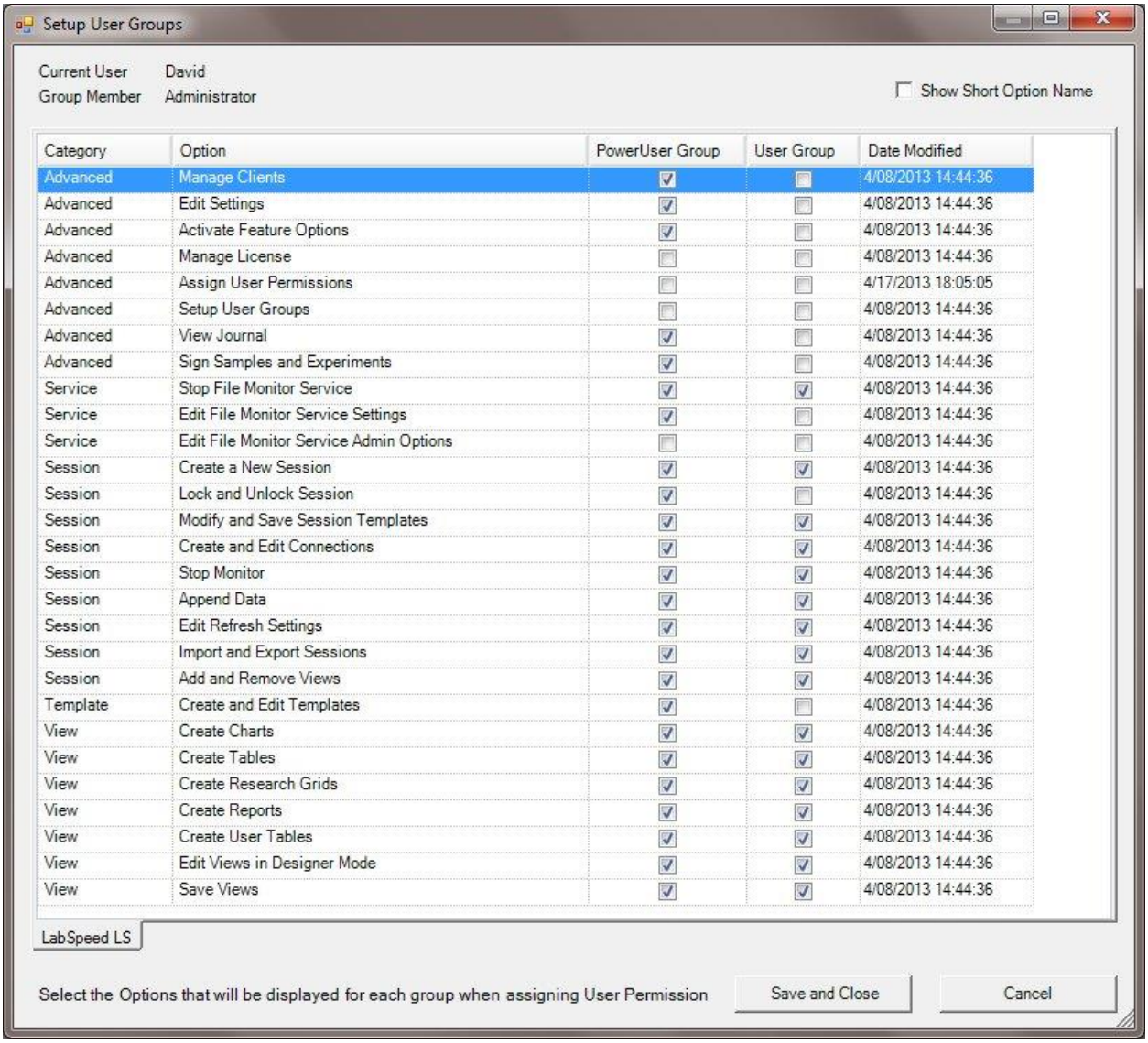
1. Administrator
2. Power User
3. User

Each user that uses LabSpeed is assigned a User Group. The User Group defines the range of permissions allowed for users in that Group.

Since the Administrator always has all permissions, only the *Power User* and *User* groups may be setup. How the administrator decides to operate the lab will determine the settings in each group. For example, a *User* may be considered an instrument operator with few rights to change anything. a *Power User* may have almost all the permissions of an administrator, or he may be allowed only *User* rights plus additional modification rights, such as changing and editing Templates and Views. It is up to the Administrator.

A user's permission set may be further customized when setting individual user permissions that will be a subset of the permissions allowed by his Group.

Click on the *Admin->Setup User Groups* menu item. The following dialog is displayed:



The above list represents all of the permissions that may be assigned to each user when logged into LabSpeed. Permissions come in five (5) organizational categories -- Advanced, Service, Session, Template and View. Note in the example above the *Power User* has many of the rights of the Administrator except a few, which include managing the LabSpeed license and modifying Users. The *User* is given fewer rights. The Administrator may give the *User* even fewer rights, e.g. to not allow creating and changing charts and tables. The rights for each group will be setup for how the Administrator will want to run the lab.

Note: If a *Power User* has permission to edit the permission groups, he/she is not allowed to change the permissions for his own group. For example, if a *Power User* is given permission by the Administrator to setup user groups, the *Power User* will only be able to change the Group settings for the *User* group.

Viewing the Journal

A journal is maintained to keep track of who is running LabSpeed and any changes to his/her status.

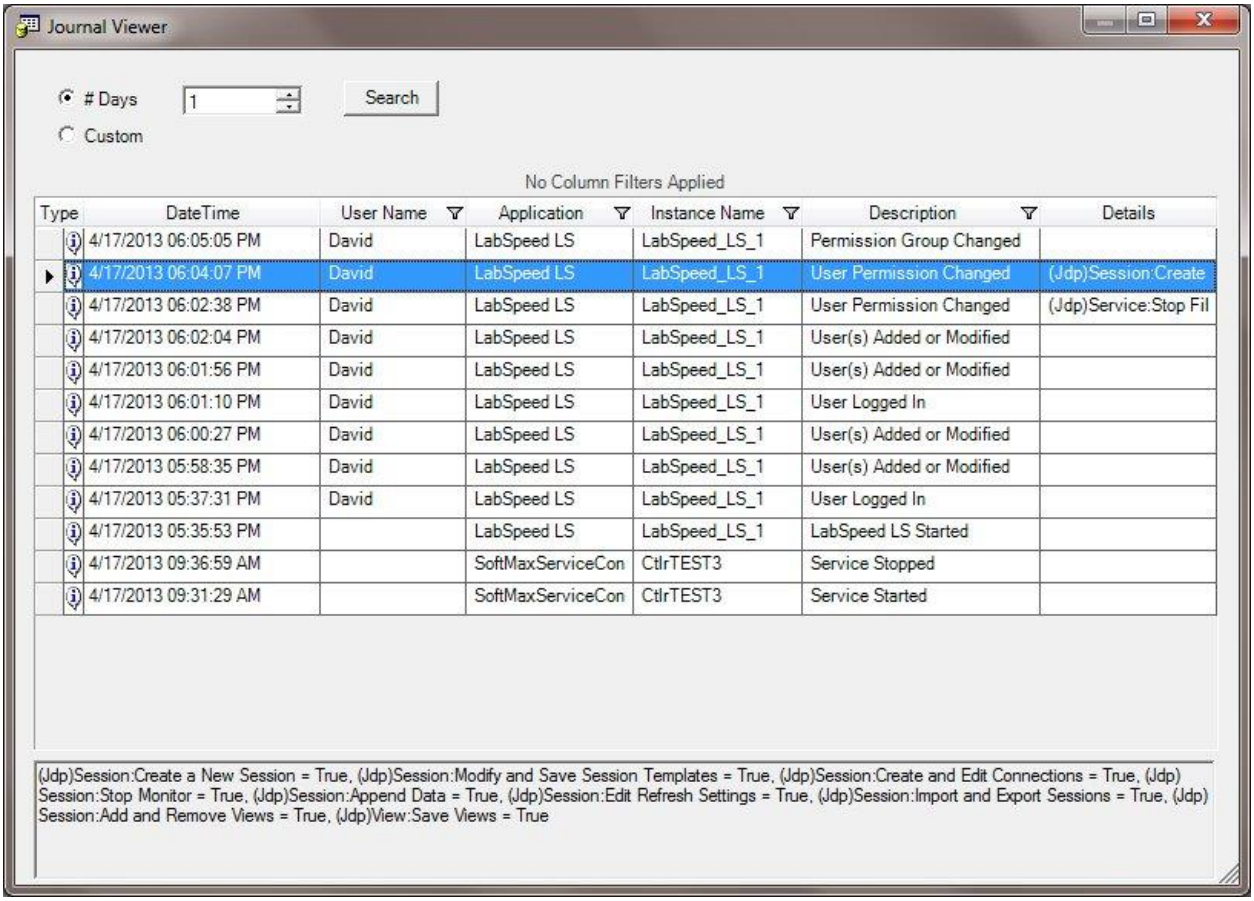
in LabSpeed

- When LabSpeed is started and closed
- When someone logs on or off
- When a User Group changes and what the changes are
- When permissions for a user changes and what the changes are
- When System Options are changed and what the changes are
- When Monitor is started or stopped
- When a Monitor status error occurs

In the File Monitor Service (if one is employed)

- When a Service Starts or Stops
- When the Service Options are changed and what the changes are
- When Service Settings are modified
- When 21-CFR P11 Authoring is enabled, and the operator cancels or fails to sign

Click on the *Admin->Journal* menu item. The following dialog is displayed:



Each Journal entry shows the following

- DateTime - when the entry occurred
- User Name - who was logged on
- Application - application name identifies the source of the journal entry
- Instance Name - identifies the unique instance of the application, service or add-in if multiple instances are being run over a network
- Description - journal entry description
- Details - additional details, which may include what changed

Select a particular entry to show the Details in the box at the bottom. In the example above, the Journal entry indicates User Permissions changed and the details indicate what those changes were and for whom (Jdp).

To view journal entries for a different date range

By default, the Journal Viewer displays entries for the current day. To view journal entries for more days, set the value for #days and click **Search.** To specify a particular date range, click on **Custom**, set the date range required (From and To) and click **Search**.

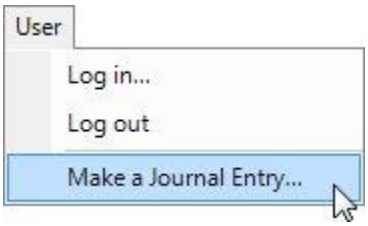
To filter journal entries to view a subset of entries

You can filter the list by User Name, Application, Instance Name and Description. Click on the "funnel" icon in the column header. A drop down list of acceptable column items is displayed for selection. You can also create a custom filter with wildcards and script logic. For example, if you filter on the Description column for "User Edit" or "Manual Journal Entry", only those entries will be displayed. Filters on multiple columns may be applied.

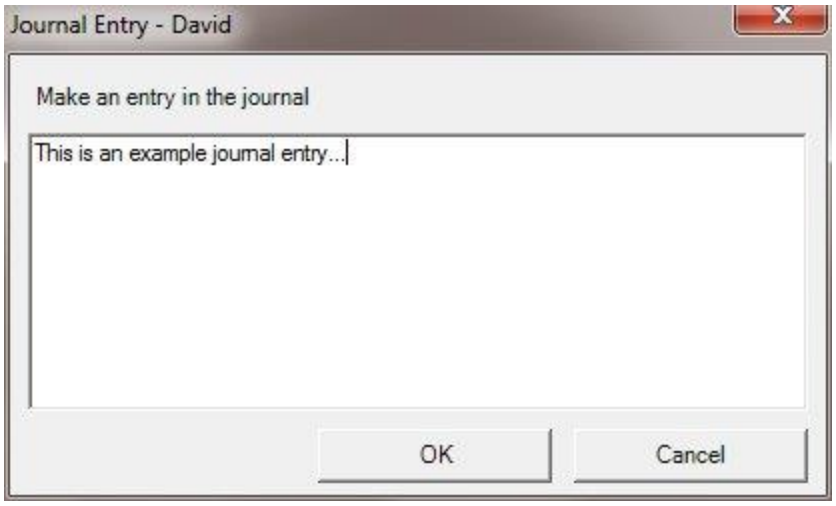
Adding a Manual Journal Entry

If the user has permission, a manual journal entry may be entered at any time. The entry is tagged by user name and date and is easily reviewed later in the Journal Viewer.

Click on the *User->Make a Journal Entry* menu item.



The following dialog is displayed:

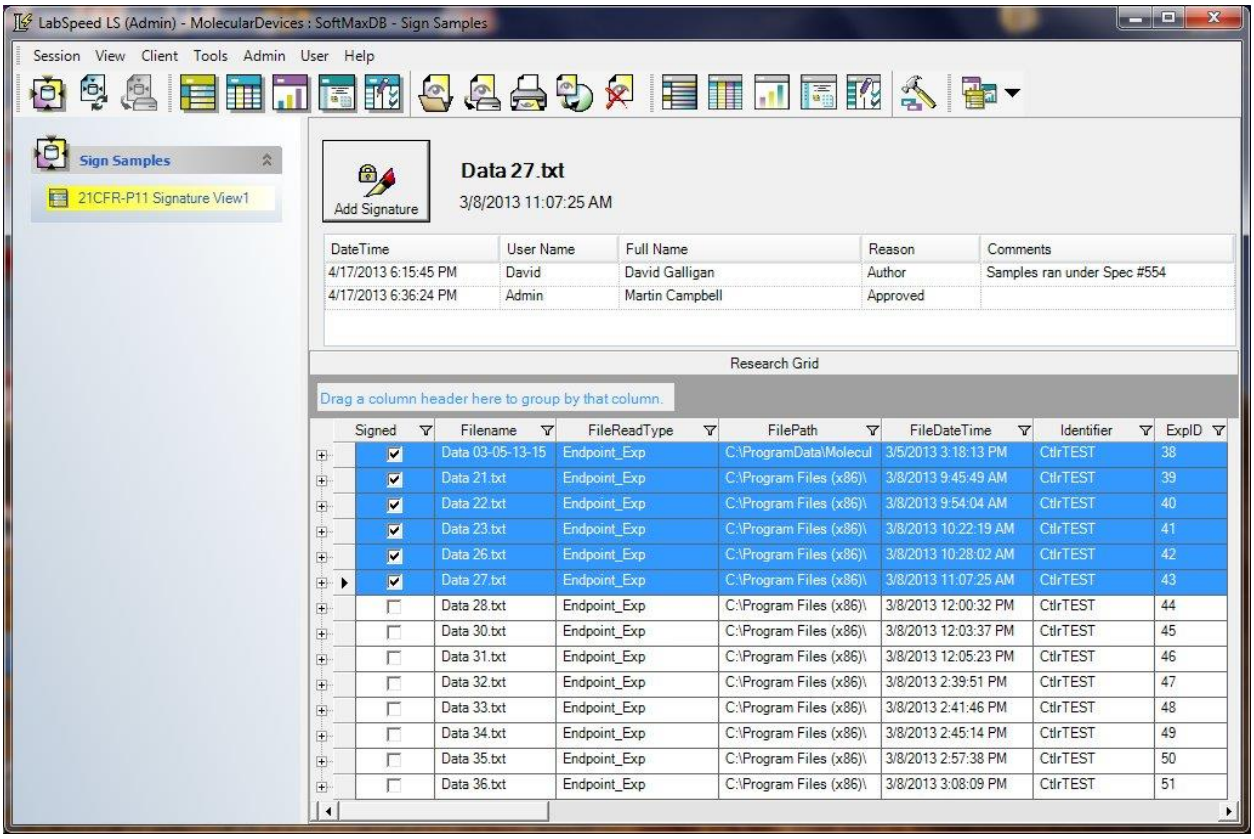


Enter any text, notes or facts and click OK.

You can view all manual journal entries in the Journal Viewer by filtering on "Manual Journal Entry" in the Description column.

Signing Samples and Experiments

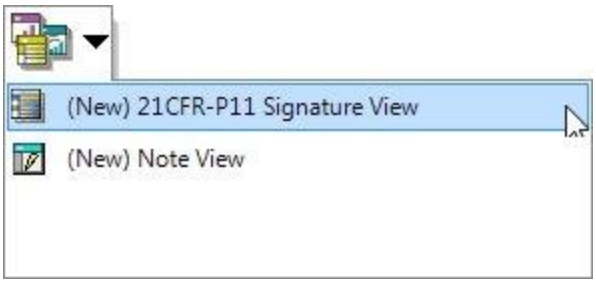
Feature Database Manager provides a special View for signing samples and experiments as *Author*, *Approved*, *Reviewed* and *Verified*. The *21CFR-P11 Signature View* may be added to any Session and saved with that Session's template.



Creating a dedicated Template for signing samples

Although the *21CFR-P11 Signature View* may be added to any Session, it is a good idea to create a dedicated Template for the purpose of signing samples, such as in the example above. The Template is called "Sign Samples" and contains a single View. You can make this Template yourself.

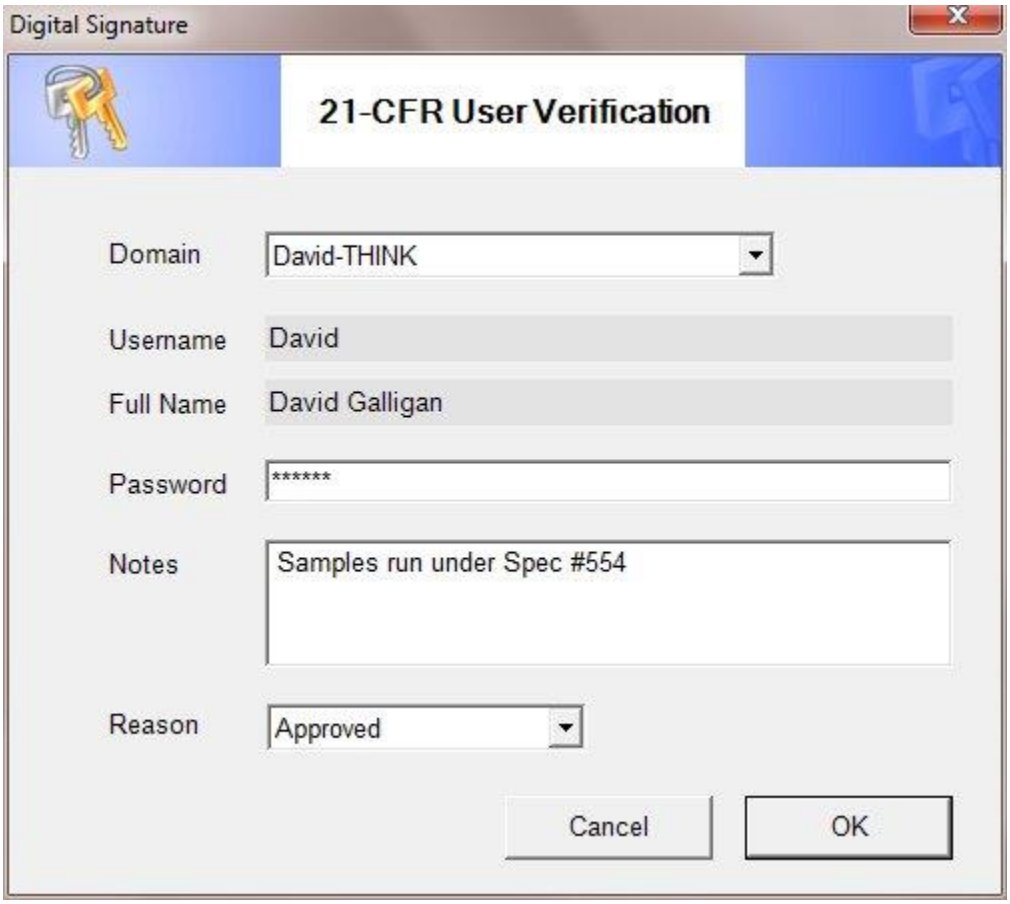
To add the *21CFR-P11 Signature View* to a Session, drop down the Special Views toolbar button and select it from the list.



To create a dedicated template for signing samples, delete all the other Views in the Session, and save the Template as "Sign Samples". It may then be used in the future for signing samples saved to the database.

Signing Samples

To sign samples, create a new Session that contains the *21CFR-P11 Signature View* and browse for the samples you wish to sign. Once the Session is displayed, **select one or more samples from the list and click Add Signature**. The following dialog box is presented.



The logged-in username and full name are displayed. Enter the Windows account password and Domain to verify who you are and enter any notes for clarification. Select a Reason from the drop down list - *Approved*, *Reviewed* and *Verified*. Click *OK* to save. If multiple samples are selected, the same signature is applied to all selected samples.

Typically the *Author* signs at the point of data storage. However, if no other signatures have been added to the sample yet, then *Author* is allowed and will appear as a selectable item in the Reason drop-down list. There can be only one *Author* signature. However, there can be multiple signatures from different users for *Approved*, *Reviewed* and *Verified*.

Selecting a sample row shows the signatures that have been entered for that sample.

The column labelled "Signed" indicates if a sample has been signed or not (any signature added).

Adding Signature to Printed Reports

The full name of the logged-in user may be added to LabSpeed reports.

In the Report Designer, add a Text control where you would like the printed name. A good place is the page footer or page header.

Select the Text control and change the following properties -- DataField - "UserFullName", Tag - "Custom" as shown below:

LabSpeed Report Designer

When printed on the report, the user's full name will be printed at that location. For example, the page footer would look like this:

Printed by: David Galligan Page 1 of 31

File Monitor Service

Service Overview

The File Monitor Service may participate in the Security Permissions assigned in LabSpeed for each user. These permissions are

☑	Service	Stop File Monitor Service
☑	Service	Edit File Monitor Service Settings
☑	Service	Edit File Monitor Service Admin Options

Depending on the permission settings for each User, a user may or may not have the right to stop the service, edit Settings and edit the Service Options. Typically only an Administrator will be able to edit the Options.

Each time access to a permission item is requested (e.g. to Stop the Service), the credentials of the user are requested (username and password). Once logged in, the user's permission is checked and he must have permission to gain access. Once access is achieved, the user is automatically logged out.

To view the File Monitor Service window, double-click on the task bar tray icon : 

If the Feature Database Manager is installed and active, the File Monitor Service will show a new Service Options button that is used to turn on/off permission checking and also to enable Authoring Samples. The Service must be stopped in order to enable the *Options* button.

Service Options

Click on the *Options* button in the File Monitor Service window. The following dialog will appear:

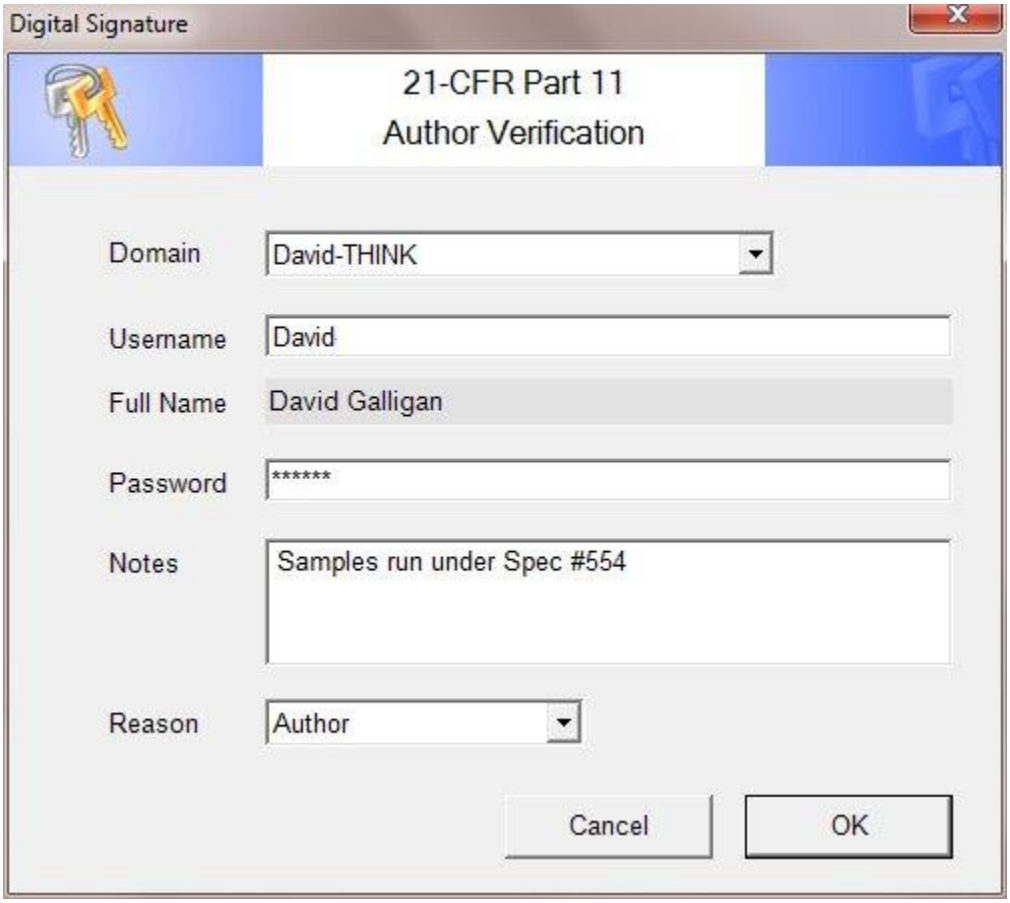
The first two options essentially enable and disable service participation in the Permissions as defined for each user in LabSpeed. When enabled, the user is required

to login and his/her permission checked before gaining access to the permission item. If not enabled, permissions are ignored and the Service can run without security as it would normally.

The third item, *Enable 21-CFR Autnor signing after saving data to database*, allows the operator to digitally sign each sample immediately after it has been securely saved to the database.

Authoring Samples

The File Monitor Service can participate in 21-CFR Part 11 signing of samples (*Author*) as they are saved to the database. If enabled, each time data is automatically imported and transferred to the database, the user will be presented the following dialog:



Enter your user name and password and any special notes and click OK. You are given 3 tries before failing to sign.

An Author's signature is not required. If the user Cancels, or fails to sign, the data be saved without an Author's signature. Later, in LabSpeed, the user may batch sign samples as the *Author.*

Note: Batch signing samples as *Author* after the fact is allowed only if it is the first signature to be added for each sample.

Index