# Peak Spectroscopy Software 21 CFR Part 11 Compliance Package

This document describes how to set up the database of users that is needed for 21 CFR Part 11 compliance.

Also see the document 'Operant_21CFR_Part_11 Compliance Statement.pdf' which tabulates the features in the Peak software which bring it into compliance.

## User Administration Program

The User Administration Program creates a user database and assigns roles to users.

The User Administration Program, userAdmin.exe, provides application program security and document traceability by allowing the maintenance of a database of users for the Spectral Sage suite of programs. Through the userAdmin program, users can be required to login when one of the $[PROGRAM] programs is started. Access to application programs is controlled, and results and reports generated by these applications can be traced back to the user.

### userAdmin provides these program access security features:

- A user ID and password are required to start an application.
- A user ID and password combination must be unique.
- There is the ability to require a password change on the next login.
- There is a configurable minimum password length.
- Users will be locked out after a selectable number of incorrect password attempts.
- A configurable inactivity timer can be enabled to automatically log a user out of an application.
- The time-out requires re-entry of a valid user ID and password in order to regain access to the application.
- A user password is not viewable on-screen when being entered.
- Passwords can be set to expire after a configurable number of days.
- Reuse of the last five passwords is prevented when a password is being changed.
- The user database is encrypted so it cannot be read by anybody.
- The user database file is protected so it cannot be easily located or removed.
- The user database file contains a checksum to detect tampering or corruption of the file.
- Access roles allow for Administrators with all system access, Super-Users with some permissions, and Standard Users with limited permissions.
    1. Standard Users are limited to running application programs. They cannot configure methods or instrument configuration files. They can only select methods and configurations created by Administrators or Super Users. They cannot access the user database.
    2. Super Users can run application programs and create and edit methods and instrument configuration files. They cannot access the user database.

3. Administrators can do everything a Super User can. In addition, they can access the user database.

- An Administrator can disable a user login.
- An Administrator can require a user to change their password on the next login.
- Only administrators are allowed to create, modify or disable users.

## Installation and Initialization

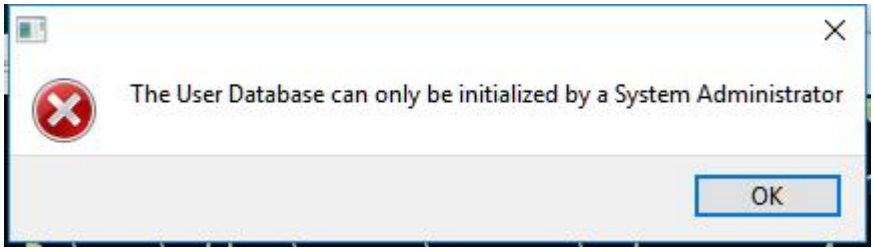
None of the security features listed above are enabled by default. After installation, the userAdmin program must be run if Application Security is to be enforced.

### *Running userAdmin.exe the first time*

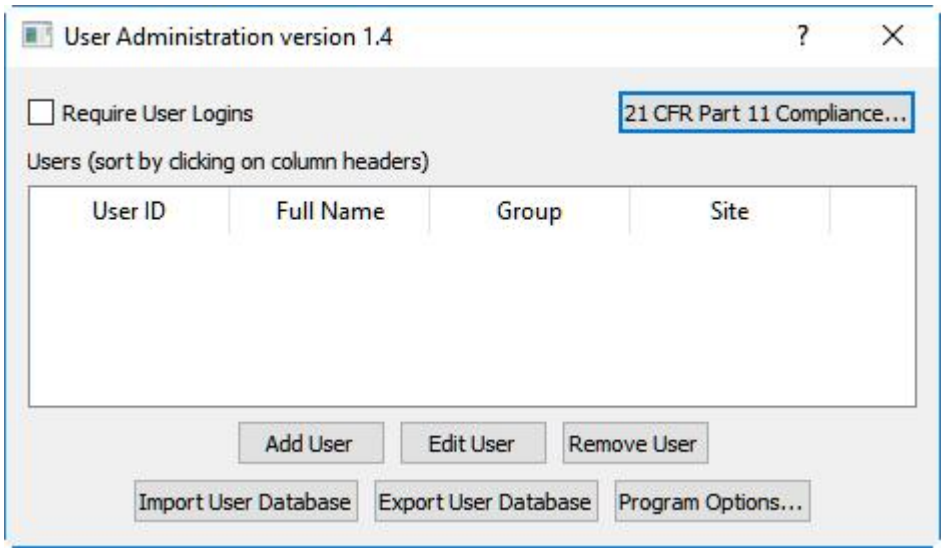
The installation program does not create a desktop icon or a shortcut to the userAdmin program. To run it, use the Windows file explorer to navigate to the folder that $[PROGRAM] was installed to.

The first time the userAdmin program is run, it must be run by a user with Windows System Administrator permissions. In addition, the userAdmin program must be run the first time by right-clicking on the program and choosing 'Run as Administrator'.

This error is displayed if a non-administrator tries to run it the first time.




When the program is launched successfully the first time, this window is displayed:




A user with Application Administrator privileges must be created before the userAdmin program can be closed. It is highly recommended that at least two different Application Administrator accounts be created. 'Application Administator' means a user that is thereafter allowed to maintain the user database. Do not confuse 'Application Administrator' with 'Windows System Administrator'. An 'Application Administrator' does not have to be a 'Windows System Administrator'.

After userAdmin is run the first time to create Application Administrators, only Application Administrators can run the program.

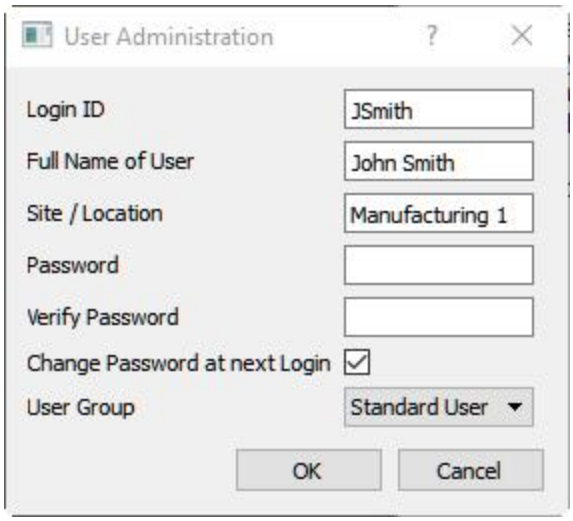
By default, User Logins are not required, so 'Require User Logins' must be checked to enable 21CFR part 11 features. **Leaving this unchecked means there is no application program security in place.**

### Important Notice about Passwords

- *Lost passwords cannot be recovered, ever.*
- *If Administrator passwords are lost, the userAdmin program cannot be accessed.*
- *There are no backdoors into the userAdmin program.*

## Adding Users

Click the ‘Add User’ button to create user accounts.



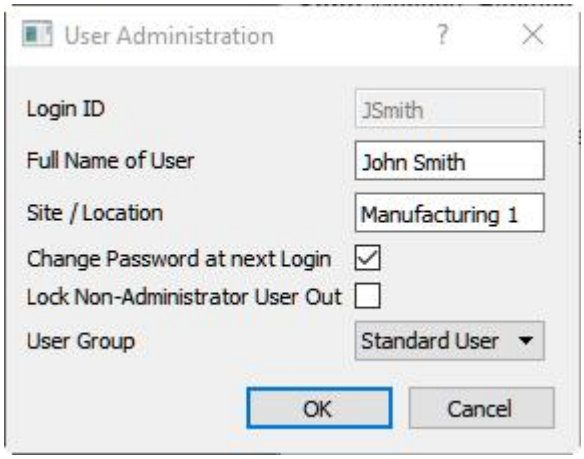

The possible choices for ‘User Group’ are:

- Standard Users are limited to running application programs. They cannot configure methods or instrument configuration files. They can only select methods and configurations created by Administrators or Super Users. They cannot access the user database.
- Super Users can run application programs and create and edit methods and instrument configuration files. They cannot access the user database.
- Administrators can do everything a Super User can. In addition, they can access the user database.

The administrator will supply a temporary password for the new user. It is highly recommended that the 'Change Password at next Login' checkbox be checked to force the user to create a new, private, password.

## Edit Users

The ‘Edit User’ button brings up this dialog:



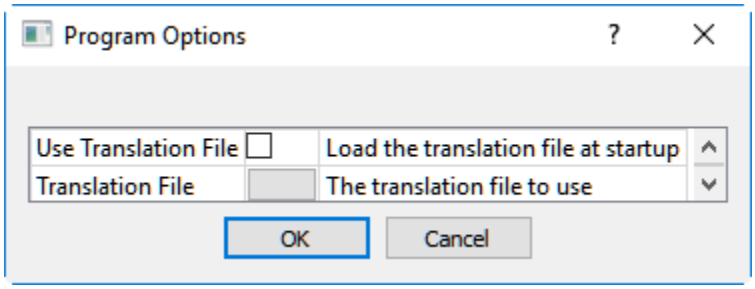

The Login ID of a user can never be changed once it is created, but other properties can. In addition, a Standard or Super user can be locked out. That is, their login will be disabled. It can also be re-enabled by un-checking that box.

Administrators cannot be locked out. To disable an Administrator, remove the user.

## Remove User

To remove a user account, select it in the Users table and click 'Remove User'.

## Program Options



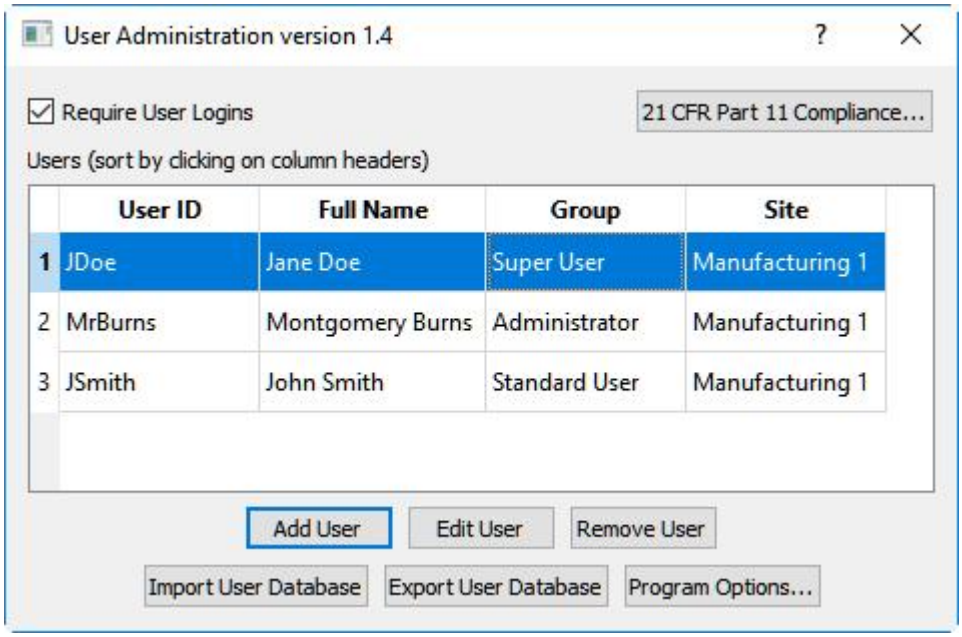

## Import and Export User Database

The 'Import User Database' and 'Export User Database' buttons allow the database to be backed up and restored. This also allows the database to be transferred between computers. The database is encrypted and tagged with a checksum, so there is no security risk in doing this.

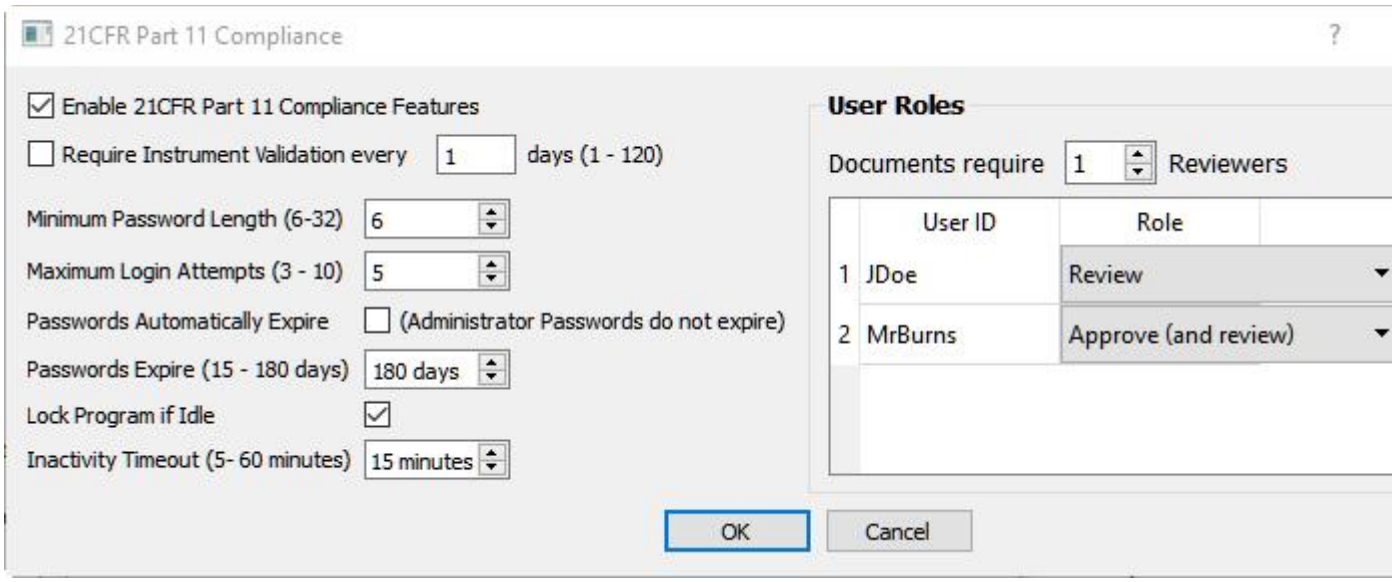
## 21 CFR Part 11

If 21 CFR Part 11 is licensed on the computer, and 'Require User Logins' is checked, the '21 CFR Part 11 Compliance' button will be enabled.

For the purpose of this tutorial, three users have been added:




Clicking the '21 CFR Part 11 Compliance' button will bring up this dialog:




*Note: For Instrument Validation, the instrument manufacturer or user must supply a validation program or procedure. Operant LLC does not provide this piece.*

## User Roles

Super Users and Administrators can be assigned roles in verifying and signing documents.

The roles that can be assigned are:

- No Role
- Review
- Approve (and Review)

Spectral data files, reports, instrument configuration files and quant methods must be reviewed and approved before they can be used in a compliant environment.

## Access Security

The options on the left side of the dialog provide Access Security. Together, these options meet the following requirements:

| | | |
|---|---|---|
| 1.1.1.1 | The System must require a user ID and password combination to log on. | Yes |
| 1.1.1.2 | The System must require the user ID and password combination to be unique | Yes |
| 1.1.1.3 | The System must allow the ability to require a password change on log-in. | Yes |

| | | |
|---|---|---|
| 1.1.1.4 | The System must provide a configurable minimum password length (at least 6 characters). | Yes |
| 1.1.1.5 | The System must provide the ability to lockout users after a selectable number of incorrect password attempts (minimum of three attempts). | Yes |
| 1.1.1.6 | The System must provide a configurable inactivity timeout. | Yes |
| 1.1.1.7 | The system time-out must require re-entry of at least one of the electronic identification components, such as password, in order to access the application. | Yes |
| 1.1.1.8 | User password must not be viewable on-screen when being entered by the user. | Yes |
| 1.1.1.9 | The passwords must be able to expire after a set number of days. | Yes |
| 1.1.1.10 | System must prevent the reuse of at least the last five passwords when the password is being changed. | Yes |
| 1.1.1.11 | The file or database table containing passwords must be encrypted so that the System administrator cannot read the password content. | Yes |
| 1.1.1.12 | System must provide access roles that allow for administrators with all system access, administrators with limited permissions, and general users with limited permissions. | Yes |
| 1.1.1.13 | Only administrators must be allowed to create, modify or disable users, groups and roles. | Yes |
| 1.1.1.14 | Only administrators must be allowed to configure the system. | Yes |