Data Security Option

Manual: MU00169-001
Revision 55

DSI ™

DSI™

Contents

Appendix C 43

Overview

Introduction

The Data Security Option (DSO), provides user access and control over the integrity of electronic records created on the Ponemah system. It can be used to technologically assist the GLP User with meeting the requirements of 21 CFR Part 11 Electronic Records, Electronic Signatures.

Note: Use of the DSO should be complemented with Standard Operating Procedures (SOPs), developed and implemented by the User's organization, in order to comply with 21 CFR Part 11 and its umbrella regulations (GLP).

Upon installation of Ponemah software and DSO, two separate applications are created: Ponemah Admin and Ponemah. Separate applications allow the User's organization to take precautions against un-authorized use of security controls and obstruction of electronic records - all security controls are maintained in the Ponemah Admin application. It is recommended that only non-Ponemah Users (such as IT personnel) have access to the Ponemah Admin application.

In the P3 Admin application, the Ponemah Administrator (or non Ponemah User) is responsible for:

- Securing the system and setting up security controls.

- Granting Ponemah Users authority to use the system.

Once a system is secured, Users are required to use two components to gain access to the system and execute electronic signatures: a valid local user account and valid Password. The system will prevent an individual who does not use these security components correctly from performing any operations in the Ponemah application.

DSO allows the ability to generate and verify electronic signatures. Electronic signing of files created during an acquisition or replay is performed automatically at the conclusion of the operation for reasons of Authorship; the file will be signed by the User who currently has authorized control of the system. Authorized Users may open a previously created file and sign the file electronically, identify the reason for signing the file (e.g.: Review, Approval, or Responsibility) and have the option of adding notes. Prior to opening a file to be signed, the user may choose to verify the file's integrity and origin. The integrity is verified by a utility, which matches the file content at the time it was created, to the content at the time of review. If a file has been modified from its original form, the system will identify the file as such.

The Data Manager function allows the User to move, copy, or delete data files while maintaining the related signature files that provide the verification capabilities. In addition, an audit trail of activities executed in Data Manager is maintained (for

more information regarding Data Manager, refer to the ***Ponemah Physiology Platform Manual***).

Installation

Introduction

The Data Security Option (DSO) can only be installed on 64-bit Microsoft® Windows 7 or Windows 10 based operating.

Installation

Note that the DSO option is installed automatically during the main Ponemah installation, there are no additional installs to perform.

Making a System Secure

Overview

After completing the main installation of Ponemah, the Ponemah system is operational but it is not considered a secured system. After installing the Ponemah software and installing the license file (with DSO enabled), the Ponemah Administrator must secure the system. Once a system is secured, the P3 User cannot gain access to the Ponemah application without a valid Windows logon account and granted access privileges set by the Ponemah Administrator.

The following is a checklist of required operations to be performed in order to correctly secure the system and control authorized access to the system:

Step 1.) System Administrator: Setting User's Windows Accounts, **P3_Users**.

Step 2.) System Administrator: Enable the **LSS_P3_Administrator** account.

Step 3.) Ponemah Administrator: Change The Administrator Password

Step 4.) System Administrator: Create Secured Directories in which the secure data will be stored.

.Step 5.) Ponemah Administrator: Secure the System.

Step 6.) Ponemah Administrator: Make changes to the **LSS_P3_Administrator** Account.

Step 7.) Ponemah Administrator: P3 Mail Slot Configuration (optional)

Step 8.) Ponemah Administrator: Setup Access Levels.

Step 9.) Ponemah Administrator: Grant Users Access to Ponemah.

Step 10.) Ponemah Administrator: Set System Security Preferences.

Step 11.) Ponemah Administrator: Export/Import Security Settings.

Setting Up Accounts and Securing Window Directories

Step 1 - Setting User's Windows Accounts – P3_Users (System Administrator)

The group membership of a user's Windows account determines a user's rights to access files created by Ponemah, when these files are accessed outside of the Ponemah environment. The rights granted to the group member will depend on the privileges granted to the group in the secure directory in which the files are saved.

NOTE: This security feature is active only when the drive has been set up for data security.

In order for user to have access to the application, they must first be added to the **P3_Users** local window account. This is done be the administrator through **Computer Management – Groups** as displayed in the image below.
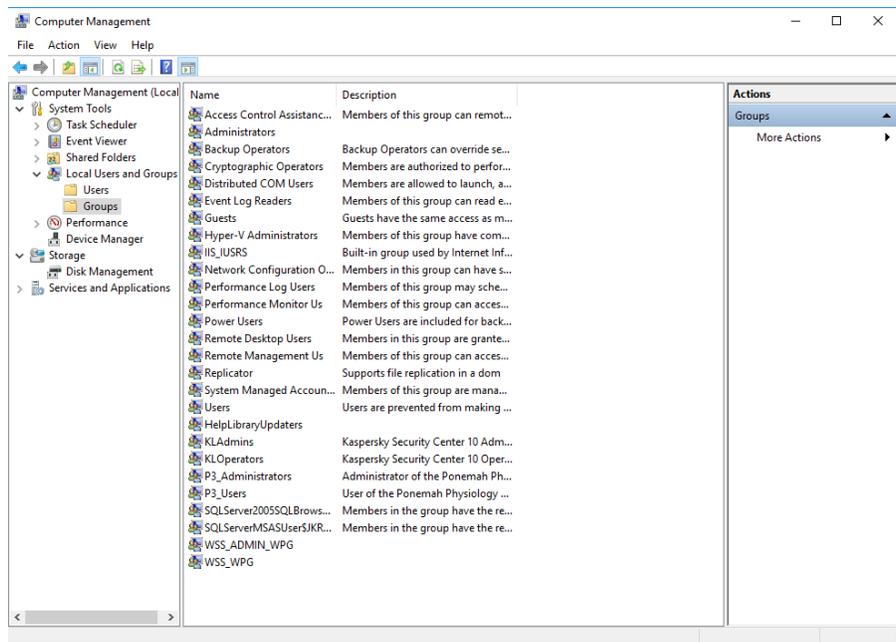
To add a user select P3_Users and select Add. The user can be from a local user account, a domain user account or a domain group.
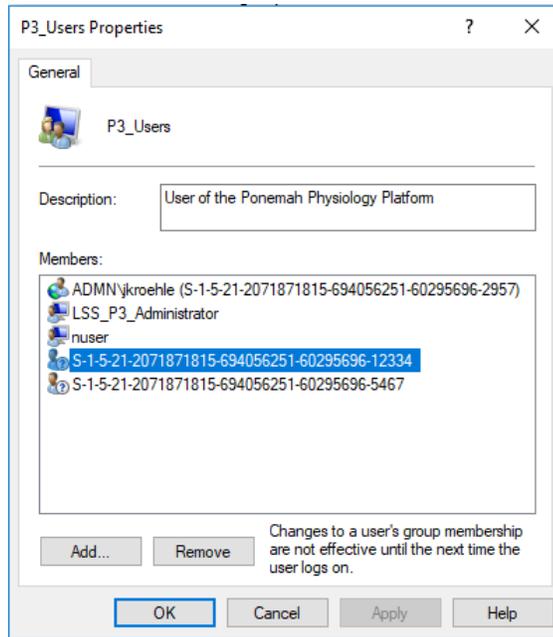
Step 2 - Enable the LSS_P3_Administrator Account (System Administrator)

The **LSS_P3_Administrator** account is created during installation with an initial password of "Gould000" and is disabled. This account is used by Ponemah for security purposes.

Right click on **Computer** and select **Manage**.

A dialog similar to the one below will appear:
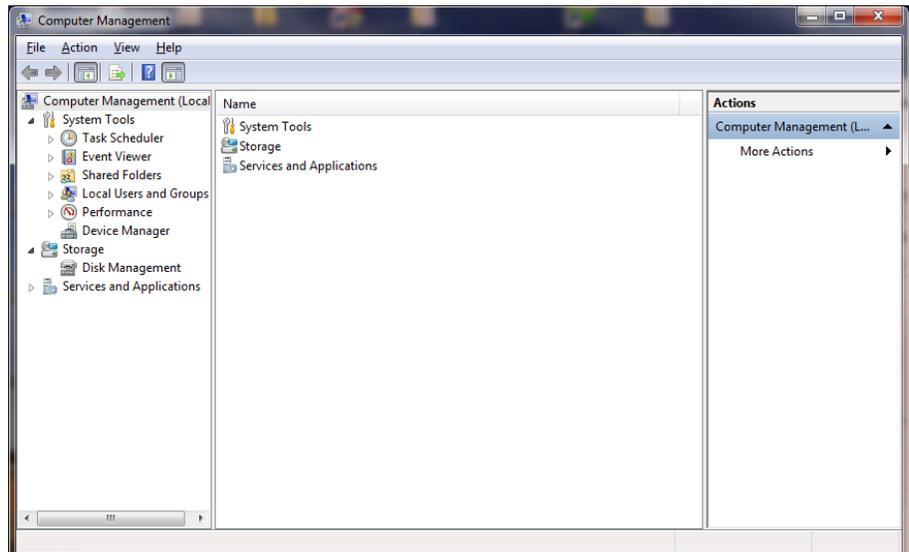
Computer Management (Local)

Select the **Users** folder underneath **Local Users and Groups**. The dialog will look similar to the one below:
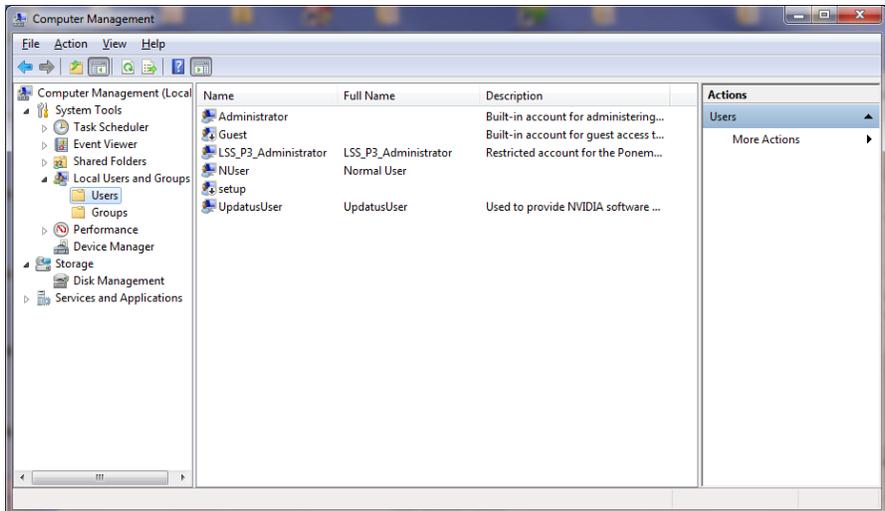
Computer Management - Users

Click on the **LSS_P3_Administrator** in the right-hand section. Click on the **Action** menu and select **Properties**. The **LSS_P3_Administrator Properties** dialog will appear:
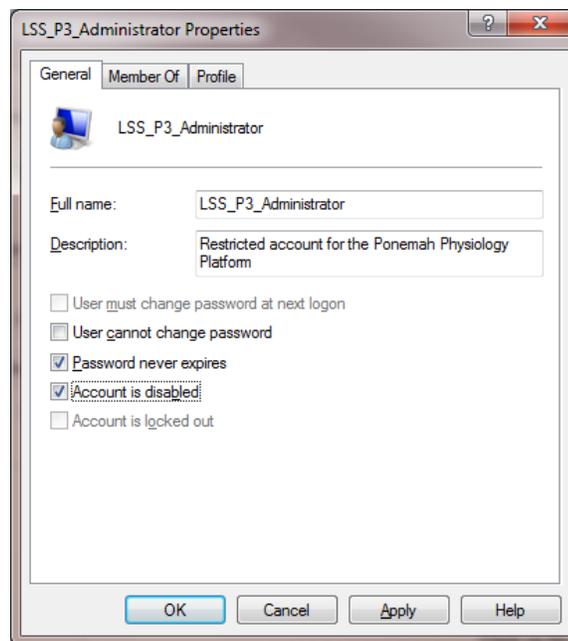
LSS_P3_Administrator Properties Dialog

De-select the **Account is disabled** check box and click on the **OK** button. Close the **Computer Management** dialog by selecting **Exit** from the **File** menu.

Restarted the computer for this setting to be applied.

Step 3 - Change the Administrator Password (Ponemah Administrator)

Ponemah Admin Application

The P3 Admin application allows the Ponemah Administrator to secure the system, set up security controls and grant Ponemah Users authority to use the system. The Ponemah Admin application is found under **Start – All Programs – Ponemah Admin**. A password is required to enter Ponemah Admin. The default Ponemah Admin password is 00000000 (8 zeros).

It is recommended that the Administrator change this password upon installing Ponemah to prevent un-authorized operations within the application. This can be done by starting the Ponemah Admin application and selecting **Change Administrator Password** from the **Tools** menu.
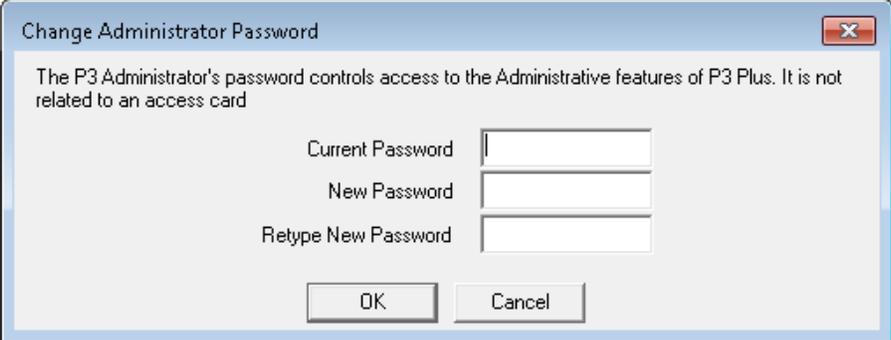
Change Administrator Password Dialog

Type in the current password into the **Current Password** text box, and the new password into the **New Password** and **Retype New Password** text boxes. Click on the **OK** button when finished.

Step 4 - Create Secured Directories (System Administrator)

These options allow the user to create and secure a new directory or secure an existing directory so that only P3_Administrators (members of the P3_Administrators group) have full access. The P3_Users (members of the P3_Users group) have read access. These selections can be selected from both the Ponemah and Ponemah Admin application. This allows the user to have the security settings configured automatically rather than having to manually configure the settings.

Creating and securing directories is listed in the application log.

Note: **Creating and securing directories can only be done on the local system.**

Creating Secure Directories

Directories can be created and secured by selecting **Create Secure Directory** from the **Tools** menu. The following dialog appears. To create and secure a directory, type in a new directory name and click on the **Create** button.

If a directory name is used that already exists, that directory will then be secured.
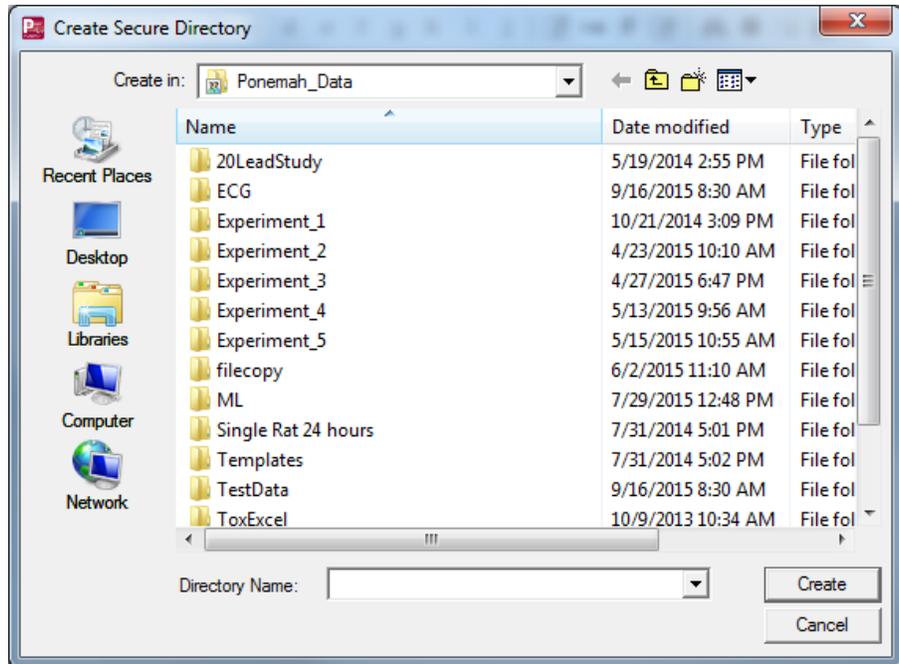
Securing Existing Directories

Directories can be secured by selecting **Secure Existing Directory** from the **Tools** menu. The following dialog appears. To secure an existing directory, select the directory to be secured and click on the **OK** button.
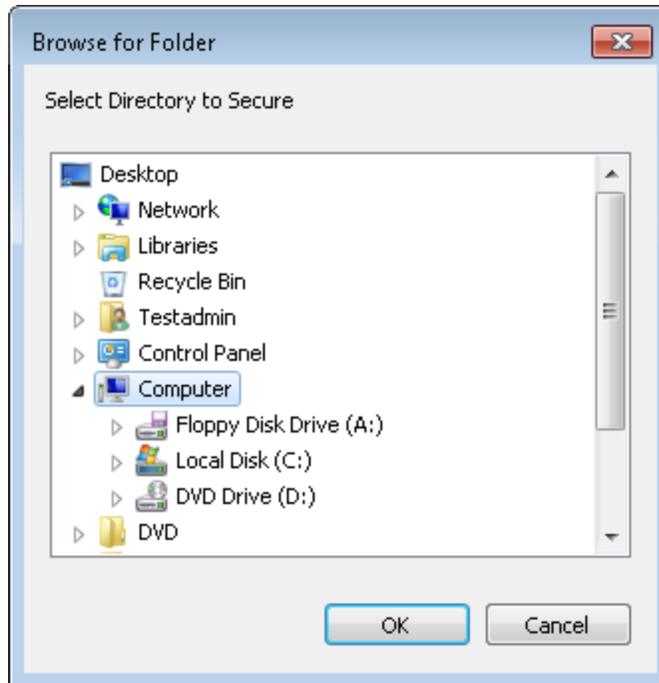
Securing Existing Directory Manually

If needed, the user has the ability to configure secure directories manually.

Create, or select, the directories in which the data will be stored. Select **Properties** from the **File** menu. For this example the directory **Ponemah_Data** will be secured. Select Properties by right clicking the mouse on the appropriate folder.

The directory **Properties** window will be displayed:
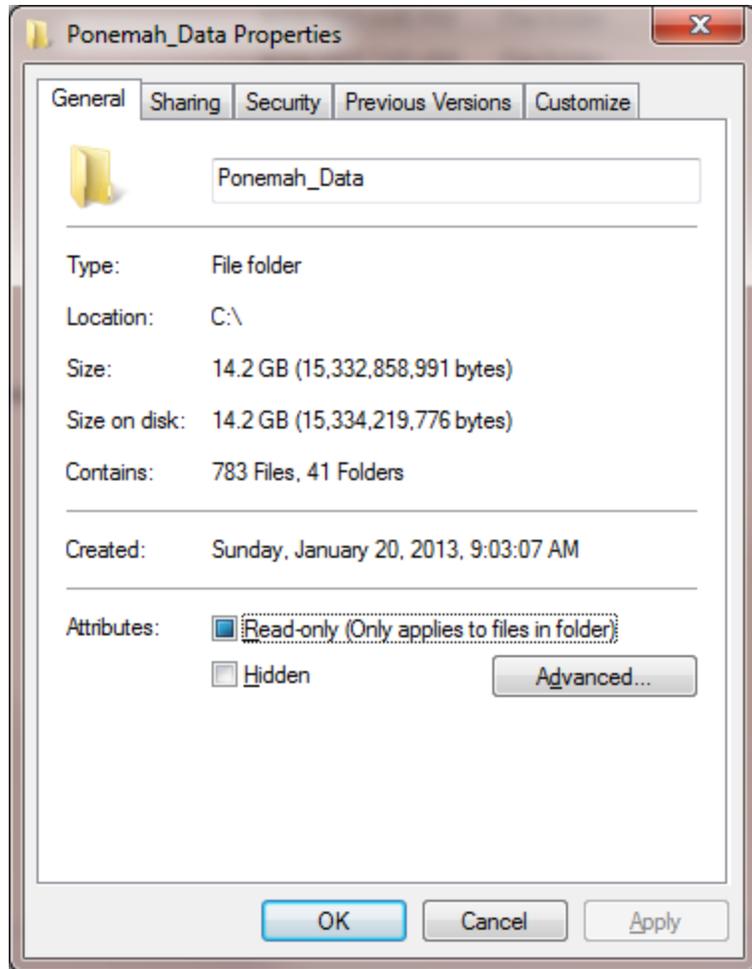
Ponemah_DATA Properties - General Tab

Click on the **Security** tab.

If the **Security** tab does not exist, see Appendix A.

The **Security** tab will be displayed:
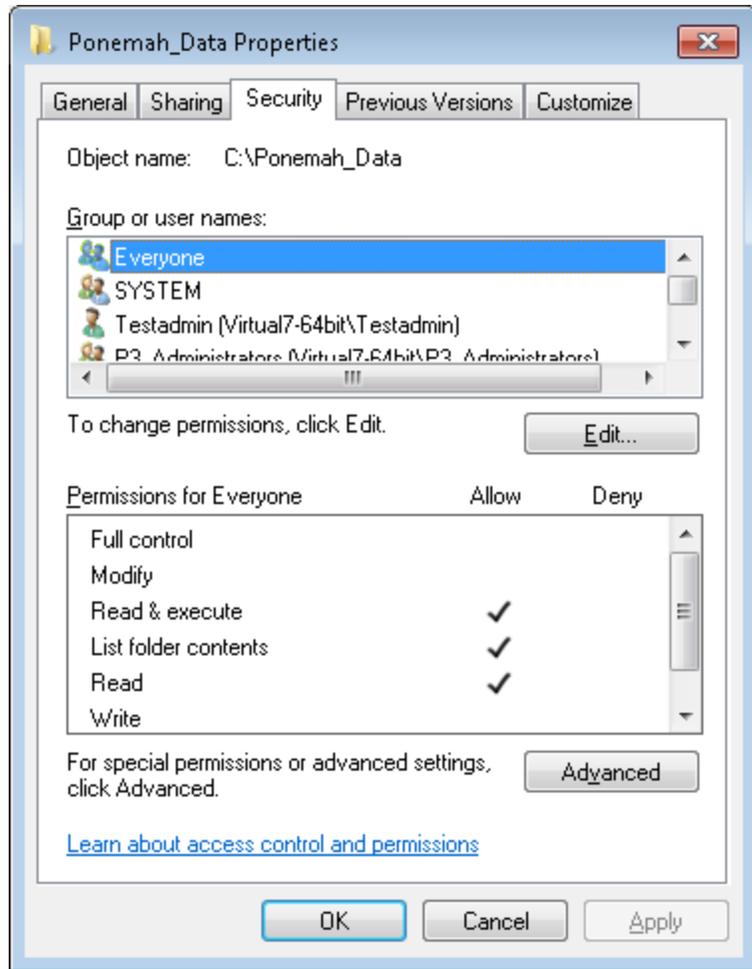
Ponemah_Data Properties - Security Tab

Click on the **Advanced** button. This will make the **Advanced Security Settings for Ponemah_Data** dialog appear:
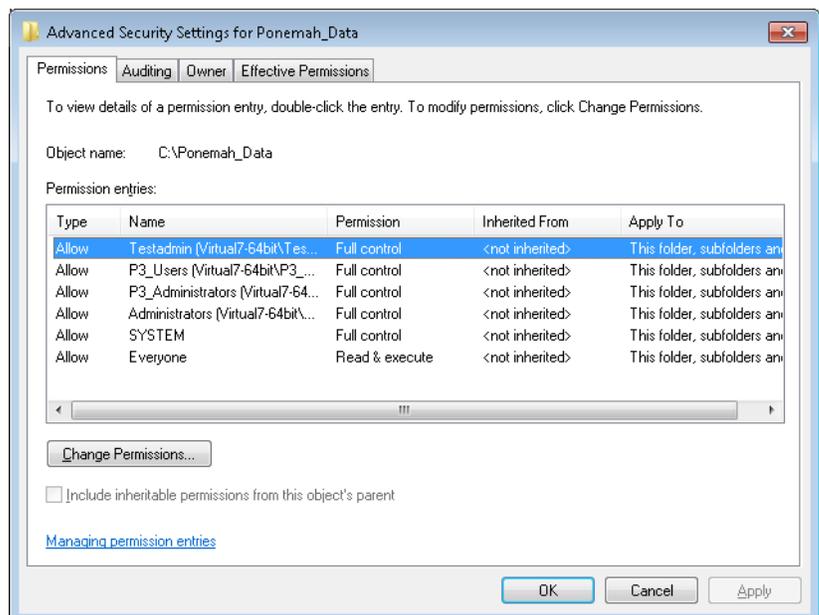
Advanced Security Settings for Ponemah_Data Dialog

Click on the **Change Permission** button. This will make the Permissions dialog appear where the user can change permissions, add and remove users or groups from the Ponemah_Data folder.
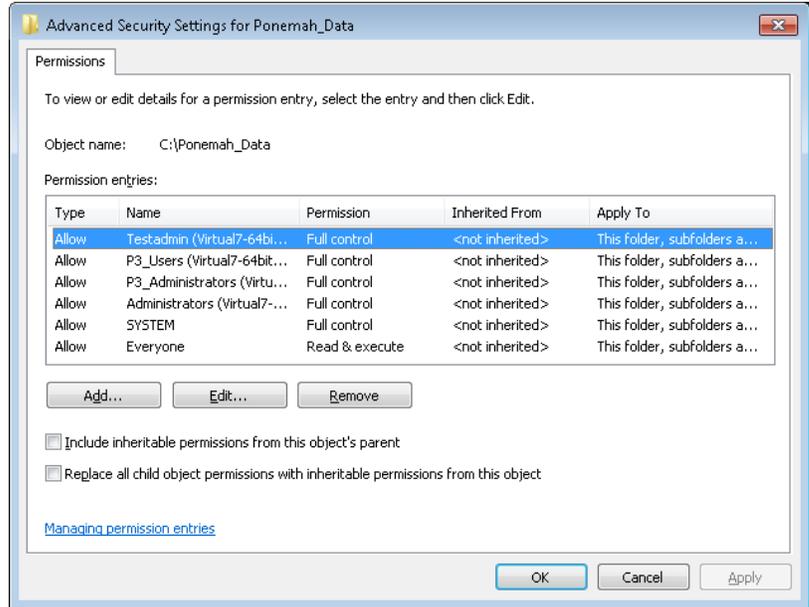
Advanced Security Settings – Permissions for Ponemah_Data Dialog

Select the **Remove** button to remove all entries except the P3_Users and P3_Administrators and the select OK twice to get back to the Properties dialog as displayed below.
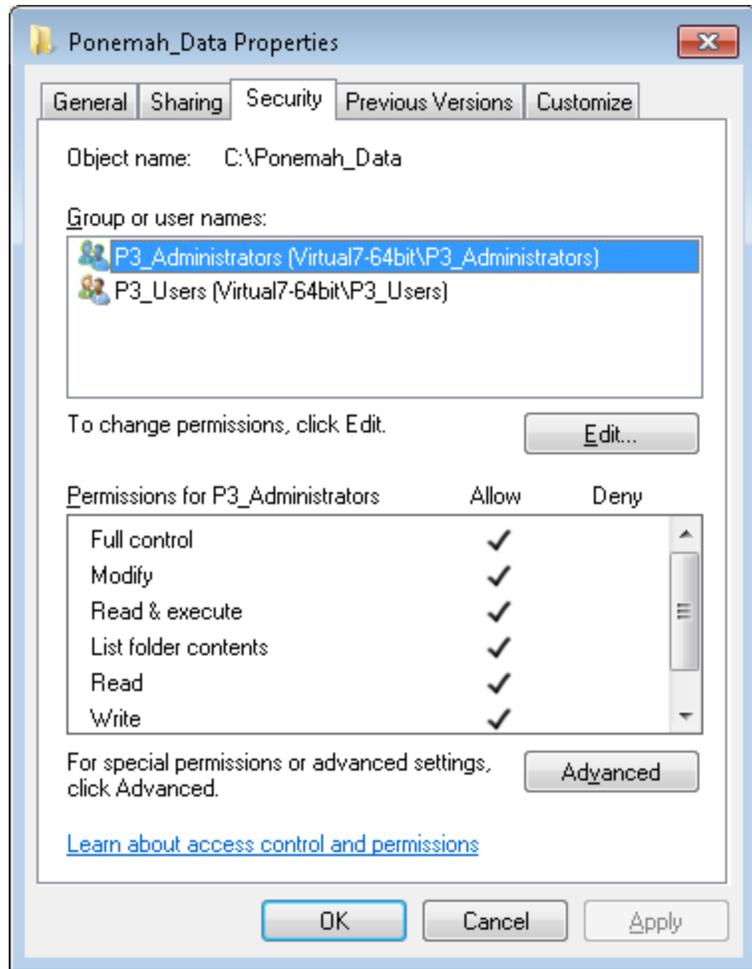
Ponemah_DATA Properties Dialog

Select the **Edit** button and this will bring up the Permissions for that folder along with the groups. Highlight **P3_Administrators** and verify that this group has **Full Control** (which is the default setting).

Next highlight **P3_Users** and modify the group only to have the following permissions: **Read & Execute**, **List Folder Contents**, and **Read**.
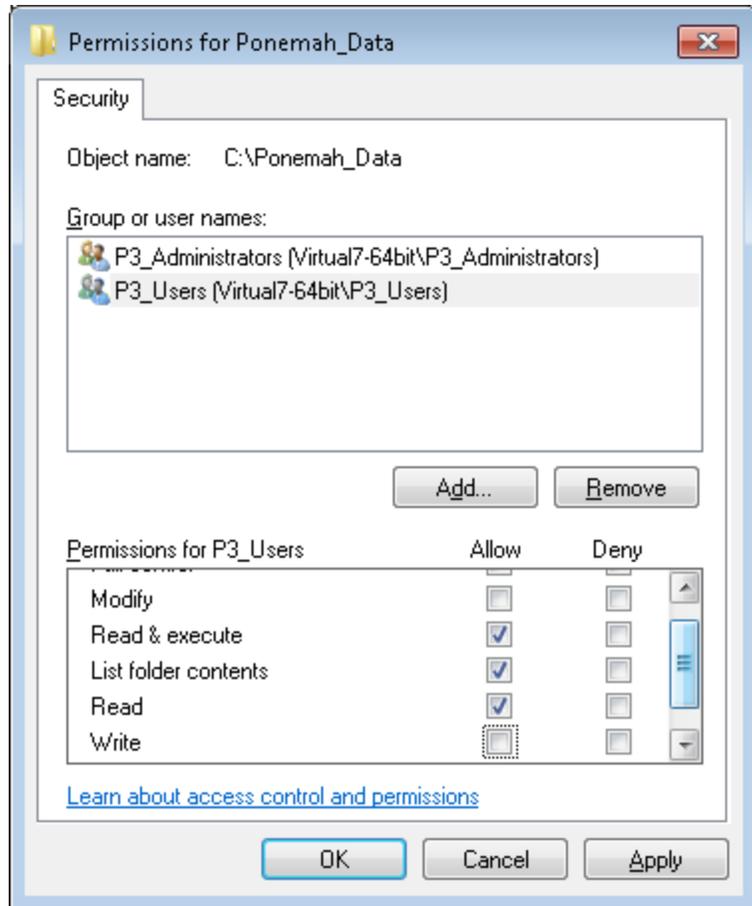
P3_User Permissions

Click on the **OK** button.

The directories are now secure.

If other groups/users need access to these directories, contact your IT department.

Step 5 - Secure the System (Ponemah Administrator)

Under the **Tools** menu, select **Make System Secure** (from within the **Ponemah Admin** application). The following dialog will be displayed.
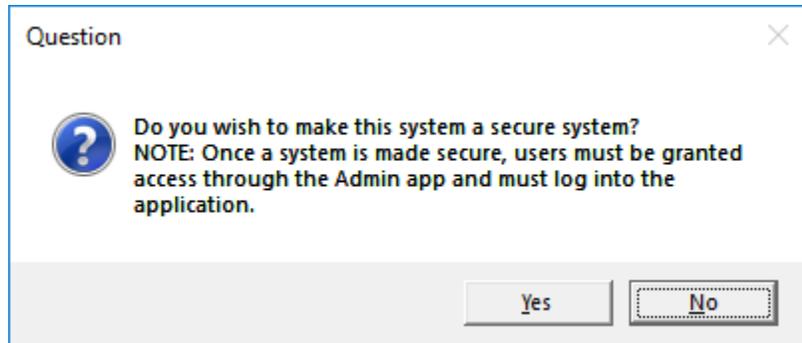
Secure System Dialog

Click Yes to secure. Once a system is secured, it cannot be accessed without the software license file with DSO enabled, and a valid Windows user account that is in the P3_Users local group. The system can be unsecured by the Ponemah Administrator. See Appendix D "Unsecuring System" for details.

Step 6 - Make Changes to the LSS Administrator Account (System Administrator/Ponemah Administrator)

If Ponemah data is going to be copied using Data Manager or if data is going to be saved across the network, then the P3 Administrator needs to configure the settings to allow Ponemah access to the network. Create the directory where the data is going to be stored and set up the account to have to have write access (the default Account Name is **LSS_P3_Administrator**). In the P3 Admin application, configure Ponemah to allow the application access to the network using the **Change LSS Admin Account Info** dialog. The **Change LSS Admin Account Info** allows the Ponemah Administrator to configure the Account Name, Domain, and/or Password associated with the account. Upon setting up the configuration, the **Test Impersonating Administrator** button will allow verification of the defined settings.

The **Change Acct Password** button will automatically change the password in Windows (if permitted by the organization's network security controls). Changing the **LSS_P3_Administrator** password is not required, but it is recommended. If the **LSS_P3_Administrator** password is not changed, the system may be vulnerable to a logon attempts using the default **LSS_P3_Administrator** password. When setting up the password, make sure to set it up so that the password never changes. If the password is not the same as the one that is set up through Ponemah, Ponemah will be unable to access the network.

If you plan on moving or copying data through Windows Explorer, user accounts need to be set up by the network administrator with access to that directory.
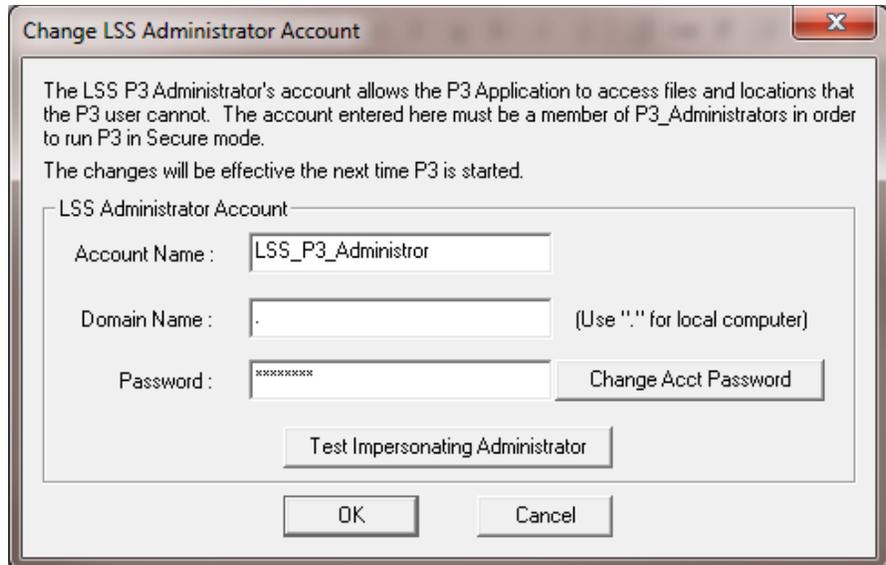
Change LSS Administrator Account Dialog

- **Account Name** - This edit box allows the Ponemah Administrator to enter the Administrator Account Name.

- **Domain Name** - This edit box allows the Ponemah Administrator to enter the Domain Name the Administrator Account is on.

- **Password** - This edit box allows the Ponemah Administrator to enter the Password for the Administrator Account.

- **Change Acct Password** - This button will open up a dialog used to change the Password in Windows, if Windows security attributes will allow it.

  o **Enter Accounts Old Password** - This edit box requires the user to input the current password for the Administrator's account.

  o **Enter Accounts New Password** - This edit box allows the Ponemah Administrator to enter a new Password.

  o **Retype Accounts Password** - This edit box allows the Ponemah Administrator to re-type the new Password to ensure accuracy.

- **Test Impersonating Administrator** - This button will use the current Name, Domain, and Password and attempt to login to the account, used for verification purposes.

NOTE: If the impersonation fails check that the P3Service is running otherwise the application cannot perform the impersonation.

Step 7 - P3 Mail Slot Configuration (Ponemah Administrator – optional step)

P3 Mail Slot Configuration Dialog

This dialog allows the configuration of the P3 Mail Slot. The name created with the mail slot is **P3_mailslot**. The user has the ability to define either a computer name for sending the mail slot message or the entire domain. The form of the name is:

- *\\ComputerName***\mailslot**\P3_mailslot - this sends the message to a single computer

- *\\DomainName***\mailslot**\P3_mailslot - this sends the message to a domain

- *****\mailslot**\P3_mailslot - this sends the message to everyone

To configure the mail slot notification on a Ponemah system, set the **Location** to the current domain/workgroup in the **P3 Mail Slot Configuration** dialog and click on the **Apply** button.

To test that the Ponemah Mail Slot has been correctly configured, start the P3 Mail Reader application on the computer(s) connected to the domain/workgroup and click the **Test** button. The connected computer that has the P3 Mail Slot Reader application running will have an entry listed as "Test Message from serial number: xxxx." where the xxxx is the serial number of the system that generated the message. In addition, if the P3 Mail Slot application was configured for an alarm sound, then the alarm will be heard during the test.

Step 8 - Setup Access Levels (Ponemah Administrator)

Access Levels allow the Ponemah Administrator to limit access to specific functions in the Ponemah System (see Appendix B), therefore, allowing Ponemah Administrator to further define the degree of authority granted to the User. When the User logs on, the system will recognize the User's assigned Access Level and will not allow the User to perform any of the restricted functions (i.e., the features will grayed or the system will prompt the User that they cannot perform the operation they are trying to execute). Access Levels are defined from the **Setup Access Levels** dialog located under the **Tools** menu in the Ponemah Admin application.
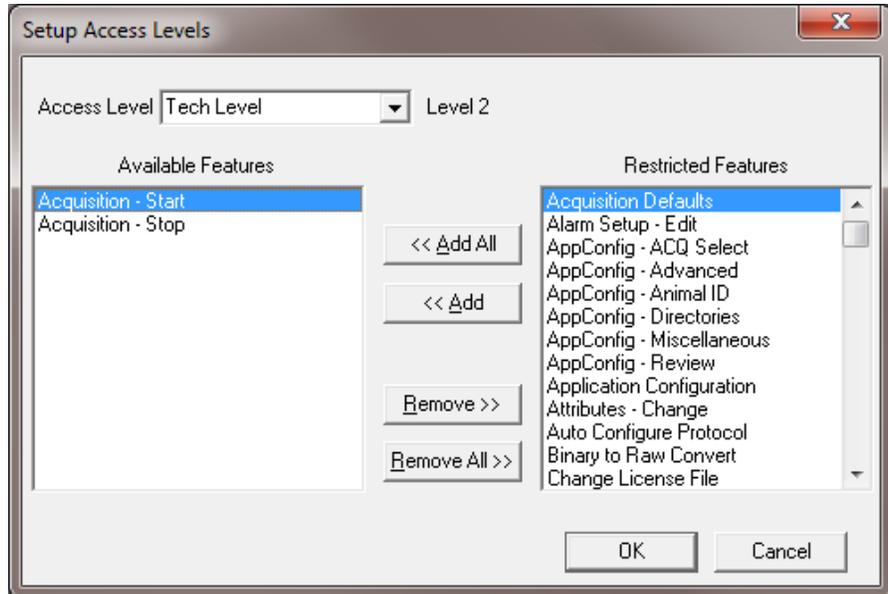
Setup Access Levels Dialog

In the **Setup Access Level** dialog, the Ponemah Administrator defines the following:

> **Access Level** - This combo box allows the Ponemah Administrator to type a name that defines the Access Level, for example, Technician, Researcher, or Lab Administrator.

> **Available Features** - This section allows the Ponemah Administrator to list the features that the User will have access to for the selected Access Level.

> **Restricted Features** - This section allows the Ponemah Administrator to list the features that the User will not have access to for the selected Access Level.

> **<<Add All/<<Add** - These buttons allow features to be moved from the Restricted Features list to the Available features list either by adding all features or by adding each selected feature, respectively.

> **Remove All>>/Remove**>> - These buttons allow features to be moved from the Available Features list to the Restricted Features list either by removing all features or by removing each selected feature, respectively.

> **NOTE: Depending on certain options installed and the acquisition interface that is selected, certain features may not be available.**

Step 9 - Grant Users Access to Ponemah Features (Ponemah Administrator)

The User's Access Card's User ID must be added to the system's User List in order for the system to recognize the User's Access Card. If there are multiple systems in a lab, then the User ID must be added to the User List and an Access Level must be assigned for each User on each applicable system they are permitted to use.   Up to 400 Users may be added to a User List.

The User List is defined from the **Setup User List** dialog located under the **Tools** menu in the Ponemah Admin application.

Setup User List Dialog

User Name - This allows the Ponemah Administrator to either select from a list of user that were entered into the P3_Users account or type in the name of the User who is being granted access to the system. This name must be a local user account or domain account name. Typically it is the User Name associated with logging onto the computer.

Full Name – is the descriptive name of the user.

Access Level - This combo box allows the Ponemah Administrator to assign an Access Level to the User.

Add - This button allows the Ponemah Administrator to add the User to the User List once the information for **User Name**, **User ID** and **Access Level** have been defined.

Update - This button allows the Ponemah Administrator to redefine information for a User who has already been added to the User List. For example, if the User's Access Level changes, then the Ponemah Administrator highlights the User in the **Current Users and Access Levels** section, changes the Access Level and then clicks on the **Replace** button.

Delete - This button allows the Ponemah Administrator to delete a User from the User List, therefore, preventing the User from gaining access to the system.

Current Users and Access Levels - This section lists all current Users (Name, ID, and Access Level) who have been granted authorized access to the system. The list box also lists the NT logon user name with the Activation Date at which time the user was added to the list of valid users.

Step 10 - Set System Security Preferences (Ponemah Administrator)

The **System Security Preferences** dialog provides additional (optional) security controls that the Ponemah Administrator can force upon Users.

Select **System Security Preferences** from the **Tools** menu in the P3 Admin application.
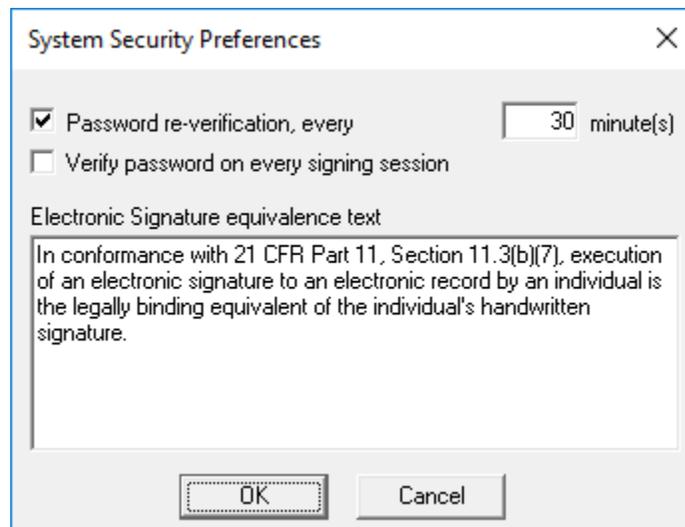
System Security Preferences Dialog

- **Password verification every x minutes** - Enabling this check box will force Users to re-enter their Password every x minutes.

- **Verify Password on every signing session** - Enabling this check box will force Users to re-enter their Password upon every execution of an electronic signature (to a group of files). If not selected, the User will be asked for a Password on the first signing only.

- **Text in the Electronic Signature equivalence text** - This text is displayed in the dialog that prompts the User for their Password (either upon log-on or when executing an electronic signature). The Ponemah Administrator has the option to edit this text according to their Company's policy.

Step 11 – Export/Import Security Settings (Ponemah Administrator)

The Export allows a user to quickly copy all Data Security settings (User List, Access Levels, and Security Preferences) defined from one workstation to another. Previously, all Data Security settings would have needed to be configured on each workstation, individually.

Export Security Settings

1. Once Export/Import settings is selected, a dialog will be displayed as shown below.
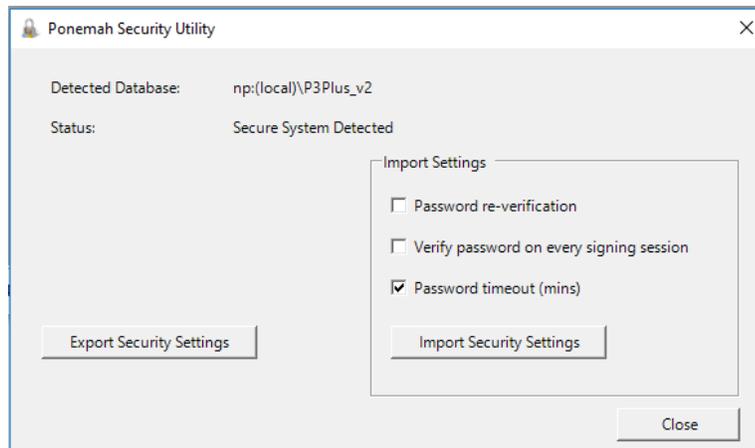
2. Click on the **Export Security Settings** to save the current security information. Note: the system must be secured to enable the Export Security Settings button.

3. Enter a file name and location for the file to be saved.

4. Click Save to create an Excel output file.

5. Transfer this Excel file to any subsequent workstation intended on having the same security settings.

Import Security Settings

The Data Security Option should be installed and functioning on the system prior to importing security settings.

WARNING: Upon importing security settings, ALL settings currently configured on the system will be deleted and replaced with the imported settings. This includes all users, access levels and other features specified during the import.

To import the security settings from a subsequent workstation:

1. Select Export/Import menu.

2. (Optional) The Import Settings menu permits additional functionality to be copied over from the original workstation that generated the export file. If checked, the function will be enabled on import and the current settings from the export file will be utilized. Each setting is described below.

    a. **Make System Secure**: If the workstation receiving the imported security settings is not currently secured, checking this checkbox will automatically secure the system.

Note: Checking this box does NOT secure any existing directories, nor does it create any new secured directories.

    b. **Password re-verification**: This will enable the Password reverification feature which will prompt the user to re-enter their Password after the designated time in minutes. This will only enable the feature but will not change the current time (in minutes) that is currently specified the dialog.

    c. Verify Password on every signing session: This will enable the feature to verify the Password upon every signing session.

    d. **Password Timeout (mins)**: This will copy the current time in minutes from the original workstation which generated the security settings Excel export file and update the time for Password re-verification when imported into the new workstation.

3. Click the **Import Security Settings** button.

4. Browse to the location of the Excel file that was exported from the original workstation.

5. Select the file and click **Open** to import the settings.

6. The **Get Reason** dialog will appear allowing a reason for change to be entered. The text entered here will be placed into the Application Log for traceability.
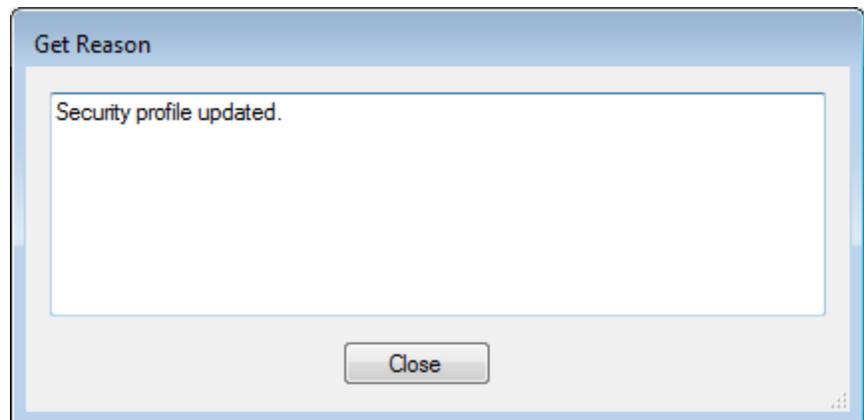
7. Click Close to save the entered reason.

8. Click OK.

Verifying Security Settings Import

Once imported, verify changes by logging into the Ponemah Admin application. View the Setup Access Levels, Setup User List and System Security Preferences menus to verify the changes were made.

All changes and the reason entered for the changes are logged in the Application Log and will be stored with the system. This log may be exported from this dialog for your records.

P3 Plus Application Logs

Local Server: np:(local)\P3Plus	Database Version: 38	Close
		Print
		Export

Application Log

Real Time	User	Action
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Time/Data Format - Setup
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Events - Label
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Digital Display - Setup
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Graph Page - Setup
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Alarm Setup - Edit
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Derived Parameters - Select
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Attributes - Change
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Input Setup - Edit
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Protocol Header - Edit
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Printer Setup
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Protocol - Save As
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Protocol - Save
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Feature Protocol - Open
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Level ID Level 1
2016/08/12 13:38:46	ADMN\ch...	ADMIN: ACCESS LEVEL: Access Levels deleted

Using DSO

Authorized Access to Secured Systems

The Ponemah Administrator is responsible for securing the system according to the installation instructions provided in this manual; a system is not considered secured until the Ponemah Administrator implements these steps. To secure a Ponemah system, the User should contact their Administrator.

Once the Ponemah Administrator has secured the system, they are responsible for granting Users authorized access to the system by assigning users to the local Windows P3_Users group account and adding the User to the system's User List. The User List defines which Users have authorized access to a system. The User List includes the User ID and the User's Access Level permitted on the system. When a User logs on to the system, the system will perform an authority check:

- Verify that a valid password for the user account has been entered into the startup dialog.

- Verify the User's Access Level on the system.

Defining Controlled Access to the System

Once the Ponemah User has selected the user name from the drop down list in the dialog and entered a valid password, the User gains control over the Ponemah System. The User is granted continuous control over the system until the User logs out of the application. Upon logging out of the application, the User, nor any other individual, will have access to the system. In order to regain control, the system will require the User to enter a valid password.

During a continuous control period, the system may require the User to re-verify authorized control of the system (optional feature enabled by the Ponemah Administrator). To maintain control over the system, the User will be required to enter a valid password for the user account. The system will not grant the User the ability to perform any operations in the system until the User has appropriately verified control.

While the Ponemah application is open, the system will allow multiple Users to log on and log off the system. The User who wants to perform any operations within the Ponemah application must selected the desired user from the dialog and enter a password appropriately.

When the application is logged out of, no individual will be able to perform any operations within the Ponemah application, even if the Ponemah application remains open. This allows Users to perform extended periods of data acquisition. During acquisition or replay mode, the system will continue to acquire or replay data

without a User maintaining control of the system and prevent any unauthorized changes to the experiment.

Logging On to Ponemah

Once a Ponemah system is secured by the Ponemah Administrator, a User will need to be in the P3_Users group and be added to the system's User List in order to gain access to the Ponemah application, and therefore, perform any operations within the application.

To log-on, select a user from the drop down and enter the password for that user.
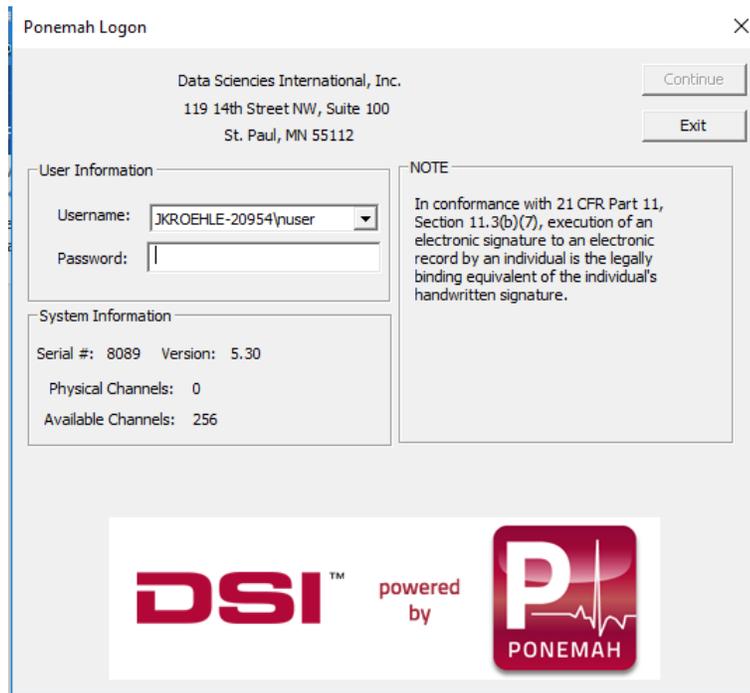
Ponemah Physiology Platform Secure Login Dialog

Upon entering a valid password, the application will open and permit the User to perform operations within the Ponemah application according to their Access Level. The User will maintain control of the system until they log out of the application by entering the key combination <Ctrl><Alt><L>.

Upon entering the Log off key combination the Ponemah Logon dialog will be displayed with the last user who logged on.

Logging Out of Ponemah

In order for the user to logout and lock the application from any changes, the user must enter the key combination of <Ctrl><Alt><L>. This will display the above Secure Logon Dialog.

Signing Files

.SIG (signature) files are used to represent electronic signatures; they contain the encrypted information required to link the .SIG file to its corresponding electronic record (the record to which the electronic signature is being executed) as well as the information that represents the User(s) digital credentials. Electronic signatures are verified for their integrity and can be viewed in human readable form using the **Verify** utility.

Note: When executing an electronic signature, the User should be aware that they might be signing groups of files (e.g. at the end of an acquisition, all files created during the acquisition are signed, such as .RAW, .XLSX, .EVT, RVW, etc).

Note: Executing electronic signatures is legally binding and equivalent to handwritten signatures.

Electronic signatures are executed under the following circumstances:

- **Signing for Reason of Authorship** - Signing will be performed automatically upon saving files and will be signed by the User who had control of the system when the files were saved. This .SIG file will have the same filename as its linked electronic record and will be located in the same directory as its linked record. Authorship will automatically be listed as the reason for signing.

- **Signing for the creation of a Parsed Review File -** Signing will be performed automatically for the RAW file created during the creation of a Parsed Review file and will be signed by the User who had control of the system when the files were saved. The resulting file will automatically be signed using the reason: Parsed. The Notes field (Verify menu) will be filled in automatically with the following information: RAW file path; Signer; Signature Time and Data; and Signature Reason.

- **Signing for Reason of Review, Approval, or Responsibility** - Users have the option to execute electronic signatures for reason of Approval, Review, or Responsibility using the **Sign File** function. Executing an electronic signature under these circumstances can only be performed on electronic records that already have a .SIG file created by the Author; the signature information is appended to the .SIG file created by the Author.

- **Signing for Reason of Initial Signature -** If a file does not have a valid signature (examples would be a file created outside of a secured system or power failure to the PC not allowing files to be signed), the software shall allow a logged in user to attach a signature to the file using the reason: Initial Signature.

- **Signing Converted Dataquest files -** Signing will be performed automatically when converting Dataquest files to the Ponemah RAW file format and will be signed by the User who had control of the system when the files were converted. The resulting file will automatically be signed using the reason: Converted. The Notes field (Verify menu) will be filled in automatically with the following information from the source Dataquest

data set: conversion type; File/Directory path; and Time and Date, if available.

- **Signing Application Log files** - When a User exits the Ponemah application, the Application Log file is signed. This .SIG file will be created in the LOG subdirectory with the same file name as the Application Log file. Note: If multiple Users gain access to the application during a continuous session, the Application Log file will maintain an audit trail of all Users who had authorized access; however, the Application Log file will only be signed by the User who exists (shuts down) the application.

Warning:
Under the following circumstances, a .SIG file will not be created for any opened files. These events will prevent the Ponemah application from creating a .SIG file and linking it to its corresponding electronic record(s), including data files and log (experimental, application, study, and review) files.

- Using Windows Task Manager (<Ctrl><Alt><Del>) to shut down the Ponemah application.

- If the system unexpectedly terminates (system crash) during use of the Ponemah application, opened files will not be signed.

NOTE:
Electronic signatures cannot be created and linked to electronic records that were originally created on non-secured systems. Even if the electronic record was replayed on a secured system, the user will not be able to execute an electronic signature.

Warning:
The Application Log files created during the use of the Ponemah Admin application will **not** be electronically signed by the P3 Administrator, and therefore, will not have an associated .SIG file.

Sign File

To execute an electronic signature for reasons of Approval, Review, Responsibility, or Initial Signature, select **Sign Files** from the **Tools** menu.
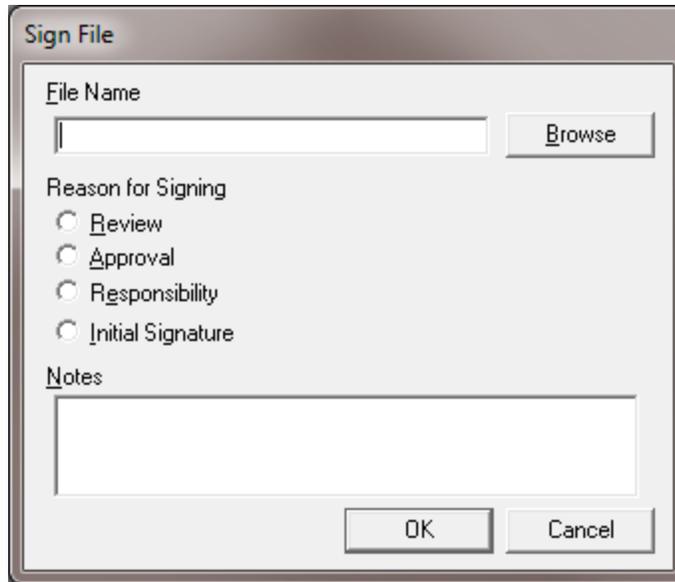
Sign File Dialog

File Name - To sign a file, select the file in the **File Name** combo box using the **Browse** button.

Reason for Signing - Select one of the radio buttons to indicate a reason for the signature (**Review**, **Approval**, **Responsibility, or Initial Signature**). The User must enter a reason for the signature.

Notes - In the **Notes** box, the User has the option of entering a message that will accompany the signature. This message will be displayed in the **Verify Files** dialog when a User verifies the electronic signature information. Entering a Note is optional.

Note:

It is recommended that the User use Data Manager when copying or moving files to new locations. The Data Manager utility maintains the integrity of the link between electronic records and electronic signatures. Upon moving or copying of files, the User should verify that the integrity of the electronic records using the Verify utility.

Verify Files

The Verify utility is used to validate the integrity of electronic files and their linked electronic signature. In addition, the Verify utility allows electronic signature information to be viewed and printed.

To verify files, select **Verify** from the **File** menu. Upon selecting **Verify**, the **Verify Files** dialog will appear.

Verify Files
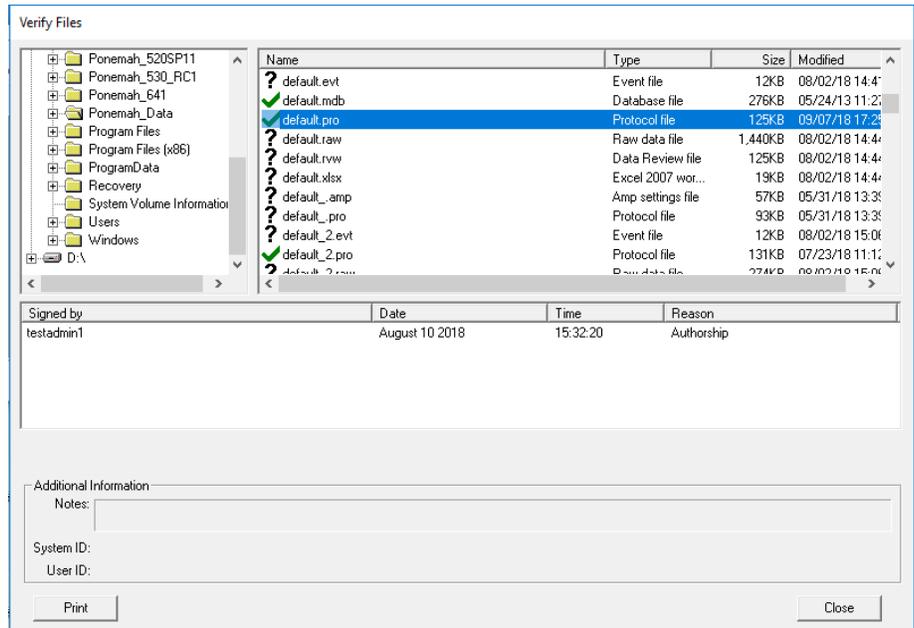
Verify Files Dialog

The User selects a directory using the tree view in the upper left section of the dialog. On selecting a directory, all applicable files are displayed in the list view to the right of the tree view. Next to each file, the validity of the file is displayed:

- *Question Mark* - Identifies a file that does not have an associated .SIG file. Under the following circumstances, a *Question Mark* will appear for electronic record(s):

  o Electronic records that were originally created on a non-secured system will not be signed.

  o If Windows Task Manager (<Ctrl><Alt><Del>) is used to shut down the Ponemah application, then the Ponemah application will be prevented from creating a .SIG file for any files that were opened when the application was shutdown.

  o If the system unexpectedly terminates (system crash) during use of the Ponemah application, then the Ponemah application will be prevented from creating a .SIG file for any files that were opened when the application was terminated.

  o If files are copied or moved outside of the Data Manager utility, then the validity of the electronic records and .SIG information may not be retained. Upon verifying records after a copy or move, a *Question Mark* will appear next to the filename in the **Verify** dialog. The Data Manager utility allows groups of electronic files, which share the same filename and signature information, to be concurrently copied or moved to the user's targeted location without impairing the validity of the electronic record(s).

  o The .RVW file will have a *Question Mark* next to its filename; however, the contents of the file can still be verified. The .RVW file is comprised of several different sub-files (see the Review Manual p/n MPNM-REVIEW for more information). These sub-

files are electronically signed, individually, and therefore have to be verified individually. To verify the integrity of the electronic records created from using the Review option, click on the .RVW file to view its sub-files. Each sub-file can then be verified for valid signature information.

- *Check Mark* - Identifies a file that has an associated .SIG file <u>and</u> the contents of the file have been verified as unchanged from initial file creation; no unauthorized changes were made to the file.

- *Cross* - Identifies a file that has an associated .SIG file, but the contents of the file have changed from initial file creation. Either the file was changed (unauthorized changes occurred outside of the Ponemah application) or the link between the .SIG file and the electronic record is corrupted.

Signed By - Lists all electronic signatures executed for the record.

Date and **Time** - Date and Time stamp of when the signature was executed.

Reason - Justification for the signature (Authorship, Review, Approval, or Responsibility).

Additional Information - Notes entered by the User during execution of the electronic signature.

System ID - Indicates which system the electronic signature (for Authorship) was created. If a file has been signed multiple times, the System ID will only be listed for the creation of the file.

User ID - Indicates which logged on user was used to generate the electronic signature.

Print - This button allows the User to produce a printout of the information displayed in the dialog.

Audit Trails

.LOG Files

.LOG files maintain an audit trail of operations performed on the system. For more information on .LOG files, refer to the *Ponemah Physiology Platform Manual*.

Audit Reason Codes

Audit Reason Codes allow the User to enter a justification for modifications made to an experiment within the Ponemah System. Audit Reason Codes may be predefined in the Audit Reason Codes dialog. The User can edit, add, or delete predefined codes that are globally or often used during an experiment. The following default codes are provided: **Administered Drug**, **Analysis not triggering**, or **Animal disturbed**.

For more information on Audit Reason Codes, refer to the *Ponemah Physiology Platform Manual*.

Print Security Setup

Print Security Setup is used to print out a list that has information regarding the Access Levels and the Access Card User ID (User) that are granted access to the Ponemah system. This feature can only be accessed through the Ponemah Admin application.

When **Print Security Setup** is selected from the **Tools** menu, the setup will be printed to the Windows default printer. The printout will list the following items:

- The date and time that the security information was printed.

- Access Levels defined on the system; each Access Level will list the permitted features that were set up.

- A list of all Users that have access to the Ponemah system. This list consists of the User Name, the User ID and the Access Level that has been assigned to the User ID.

User Log Information

In the Ponemah Admin application the administrator can view all of the administrative functions that have been performed for each of the users that have been set up for Ponemah. This is done by starting the Ponemah Admin application and selecting **User Log** from the **Tools** menu.
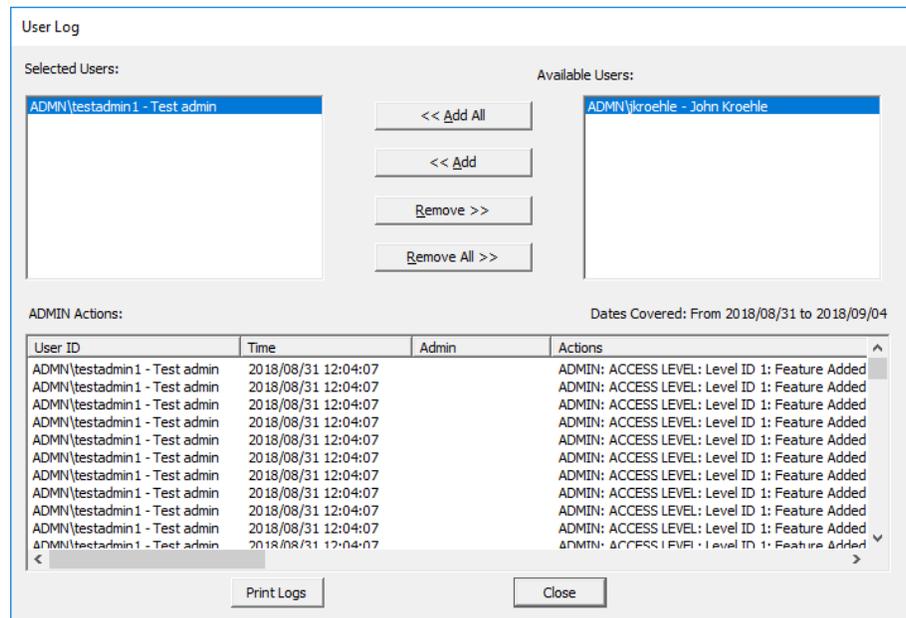
This dialog allows the Ponemah administrator to view all of the actions that have been performed for the selected users. Select one of the **Available Users** on the right hand side of the dialog and then click on the **<< Add** button. Once this is done the administrative actions will be listed in the **ADMIN Actions** section. Multiple users can be configured for to the **Selected Users** section.

The dates listed in the **Dates Covered** area are the dates from the earliest modification to the latest modification of user entries regardless of which users are selected or available.

The Ponemah administrator also has the ability to print the information listed by clicking on the **Print Logs** button. When the Ponemah administrator is done they can click on the **Close** button to close the dialog.

P3 Mail Slot

P3 Mail Slot

The P3 Mail Slot application is used to notify users/administrators of illegal login attempts to a secured Ponemah system. If an invalid password is used in attempt to gain access to the Ponemah system, the following message will be sent indicating the serial number of the system, date and time of occurrence, "ACCESS LOG: INVALID LOGIN", the User ID of the account that was used. In addition, the target computer can be configured so that a .WAV file plays when a message is received. The message may be sent to the following locations, depending upon how the P3 Administrator has configured the notification route:

- All computers connected to a domain/workgroup

- A specific computer connected to the network

The target computer must be running the P3 Mail Reader application in order to receive the message.

P3 Mail Reader

The User has the option of setting-up a .WAV file that is played on the computer when an illegal logon attempt is performed.

P3MailReader Dialog

Click on the **Configure** button in the **P3MailReader** dialog. The **Configuration** dialog will appear. In the **Configuration** dialog, click on the **Browse** button to navigate to the desired .WAV file, and select the file as the **Notification Sound**. Click on the **OK** button to select the file.
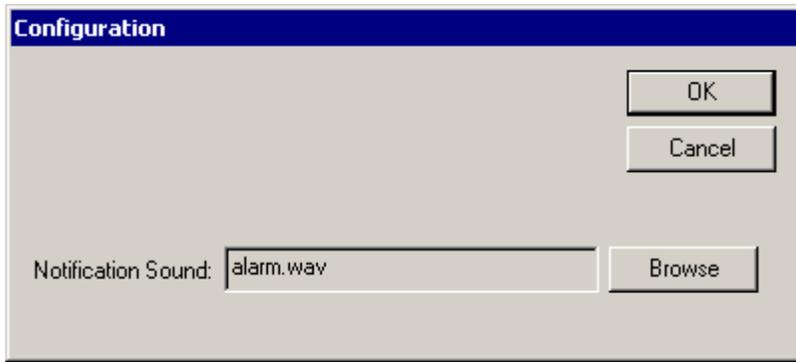
Configuration Dialog

Appendix A

Access Levels

The following functions can be selected to define each Access Level in the **Setup Access Level** dialog in the Ponemah Admin application.

Acquisition - Start	Input Setup - Edit	Review - Open Marks Information
Acquisition - Stop	JET Device Configuration	Review - Open Ref Information
Acquisition Defaults	Jump	Review - Print
Alarm Setup - Edit	Logging Rate - Change	Review - Print Setup
AppConfig - ACQ Select	Measure - Enable	Review - Save Marks Information
AppConfig - Advanced	ODBC Interface	Review - Save Parsed Review File
AppConfig - Animal ID	Options - Reason Codes	Review - Stop
AppConfig - Directories	Overwrite - Data Files	Sample Rate - Setup
AppConfig - Miscellaneous	Overwrite - Derived Files	Save RAW Data
AppConfig - Review	Overwrite - Protocol Files	Scheduler - Quit
Application Configuration	Printer Setup	Scheduler - Setup
Attributes - Change	Protocol - Open	Scheduler - Start
Auto Configure Protocol	Protocol - Save	Secure Directories
Binary to Raw Convert	Protocol - Save As	Select APR1
Change License File	Protocol Header - Edit	Select DSI Sources
Combine RAW Files	Public Key - Export	Select Digital Telemetry Implants
Data Insights - Search Definition	PV Loops - Add Analysis	SEND – Database
Data Insights - Association		SEND – Delete
Data Insights - Rejection",	Replay - Defaults	SEND - Setup
Data Insights - Edit Report	Replay - Filename	Setup 7700 Amplifiers
Data Manager-Copy	Replay - Start	Sign File
Data Manager-Delete	Replay - Stop	Study - Backup Database
Data Manager-Move	Review - Add Bad Data Sections	Study - Change Filters
Data Parser Setup	Review - Add Events	Study - Delete Study
Data Reduction - Setup	Review - Add Marks	Study - Modify
Data Set Name - Setup	Review - Add Notes	Study - New Study
Derived Parameters - Select	Review - Change X Axis	Study - Overwrite Deleted Study
Digital Display - Setup	Review - Change Y Axis	Study - Primary Workstation List
Edit Digital Telemetry Configuration	Review - Delete Bad Data Sections	Study - Restore Database
Edit DSI Setup	Review - Delete Events	Study - Run Study
Email Alert	Review - Delete Marks	Study - Save Primary Protocol
Enter Online Messages	Review - Delete Marks Information	Study-Search Path
Events - Assign To Groups	Review - Delete Notes	Study - Select Study
Events - Label	Review - Display Options	Study - Sync Entire Study
Events - Trigger	Review - Move Bad Data Sections	Study - Sync Study Data
Global Settings	Review - Move Events	Templates - Add Cycle
Graph - Change X Axis	Review - Move Marks	Templates - Analyze
Graph - Change Y Axis	Review - Open File	Templates - Delete Cycle
Graph Page - Print		Templates - Modify Binding
Graph Page - Setup		Templates - Modify Cycle
Groups - Label		Time/Data Format - Setup
Groups - Trigger Channel		Video - Online Control
Import Raw File		Video - Setup

Appendix B

Correcting LSS Administrator Account Password

If the LSS Administrator password has been changed in either Windows or Ponemah and not in the other, Ponemah will not start. The error below will appear when Ponemah is started.


If it is not known which password has changed, run through the following steps to reset the LSS Administrator password in both Windows and Ponemah.

Correcting the Passwords

The first step is to click on the **Start** button, and select **Control Panel**. The following window will appear.
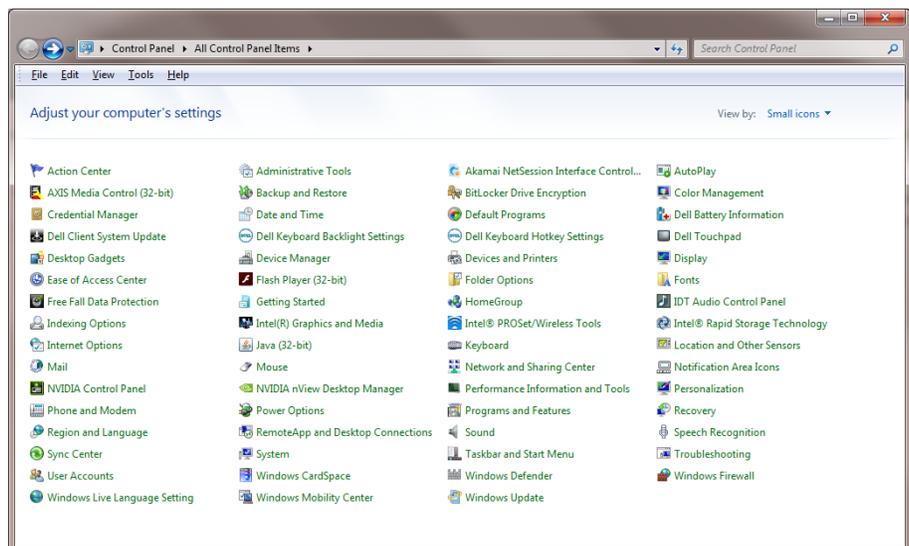

From here, click on the **User Accounts** selection.
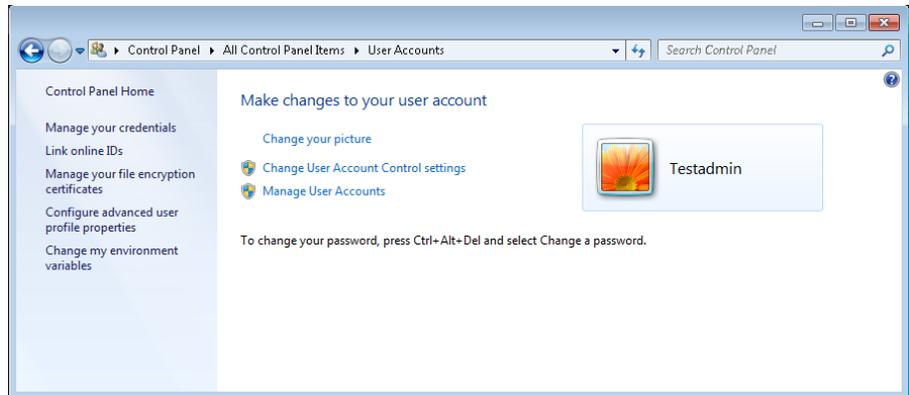
From here, click on **Manage User Accounts** selection.
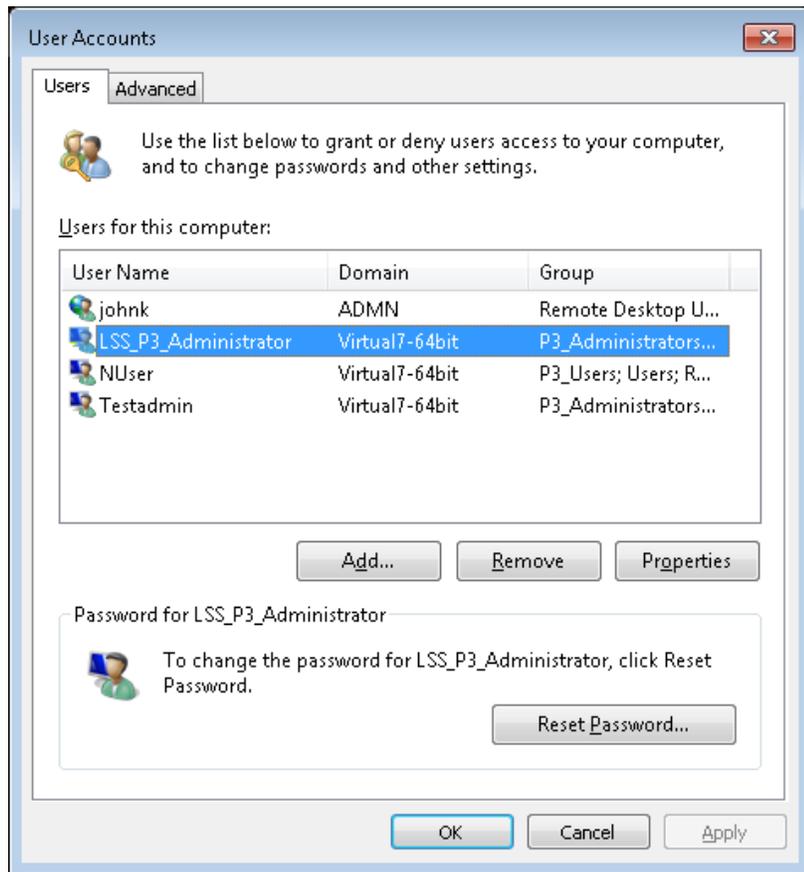
Highlight the **LSS_P3_Adminstrator** and select **Reset Password…**
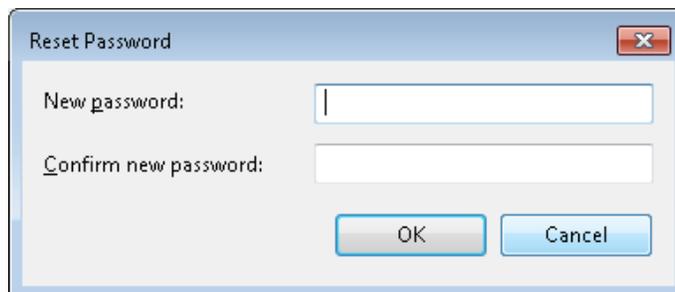
Enter a new password and then close dialog. Close the **User Accounts** dialog.
Close the **Control Panel** dialog.

Resetting the Windows password is now complete.

Start the **Ponemah Admin** application. The following dialog will appear.

Click on the **OK** button. The following dialog will appear.
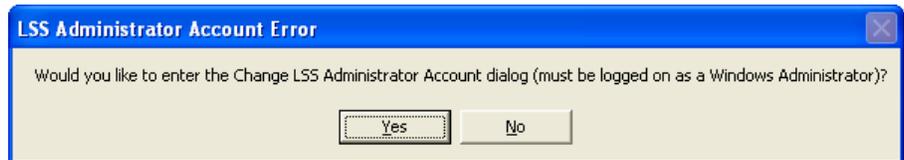
Click on the **Yes** button. The following dialog will appear.
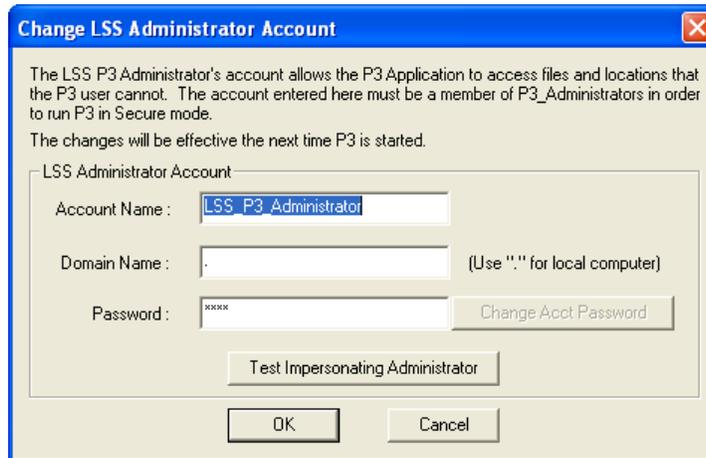
Type in the correct **Password** used above when resetting the Windows password and
click on the **Test Impersonating Administrator** button. The following dialog
should appear.

If the above dialog does not appear, the correct password that was used in Windows
was not the password typed into the **Change LSS Administrator Account** dialog or
the correct Domain is not being used.

Click on the **OK** button. Click on the **OK** button on the **Change LSS
Administrator Account** dialog.

The **Ponemah Admin** application will now start with the following dialog.

P3 Administrator Password

Please enter the P3 Administrator password for this system. This password is not associated with a user account and is specific to the current workstation.

[OK] [Cancel]
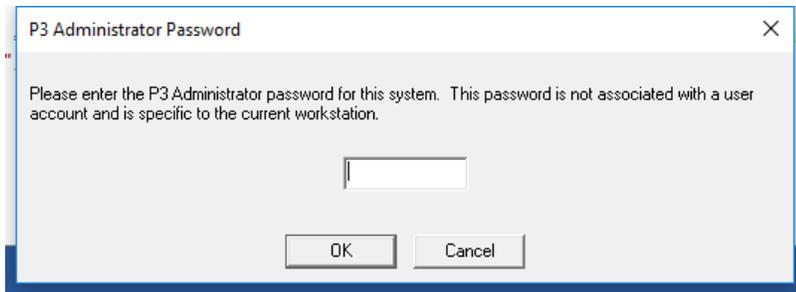
Appendix C

Unsecuring System

If the need arises, the Ponemah system can be unsecured. This can only be done by the Ponemah Administrator. This is done by starting the Ponemah Admin application and selecting **Make System Unsecure** from the **Tools** menu. Once this is done, a message will appear like the one below.
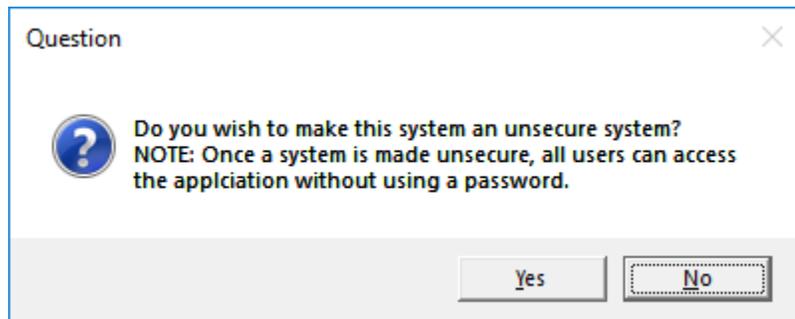
Once the **Yes** button is selected the system is now unsecured.