DSI

Data Security Option

Manual: MU00169-001
Revision 54

Data Sciences International
119 14th Street NW, Suite 100
St. Paul, MN 55112
Phone: +1 (651) 481-7400
US: +1 (800) 262-9687
Email: support@datasci.com
www.datasci.com

Data Sciences International
119 14th Street NW, Suite 100
St. Paul, MN 55112
Phone: +1 (651) 481-7400
US: +1 (800) 262-9687
Email: support@datasci.com
www.datasci.com

Contents

Overview 1

Installation 3

Using DSO 25

P3 Mail Slot 37

Overview

Introduction

The Data Security Option (DSO), in addition to Access Cards, a Card Reader, and Microsoft® Windows NTFS file system, provides 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.
- Importing Public Keys.

Once a system is secured, Users are required to use two components to gain access to the system and execute electronic signatures: an Access Card and valid PIN. The system will prevent an individual who does not use these security components correctly from performing any operations in the Ponemah application. There are several advantages to using Access Cards and PINs:

- The Access Card (sometimes referred to as a Smart Card) is a device that stores public/private keys electronically on the card. Access Cards enhance protection of a Ponemah User's electronic signature information the private key is stored on the card rather than on the hard drive. Each Access Card is initialized with a unique identification number (User ID). The User ID is used to authenticate the identity of the User; therefore, Access Cards should never be re-assigned to new Users.
  DSI/Ponemah is responsible for initializing the User ID on the Access Card; DSI/Ponemah's quality procedures ensure that no two Access

Cards share the same User ID. This User ID is electronically stored on the card and stamped on the card for visual reference.

- The Personal Identification Number (PIN) is an eight-character password used in association with the Access Card to verify that the individual has authority to use the Access Card. PINs are unique and personalized to the Ponemah User and are stored on the Access Card.
- Use of Access Cards and PINs allow multiple Users to gain access to the application during a continuous session. The application does not need to be shutdown each time a new User wants to gain control of the system.
- Data acquisition may continue without a User maintaining control of the system. If the Access Card is removed from the card reader while the system is acquiring data, acquisition will not be interrupted and no individual can perform any operations within the application. To re-gain control of the system, a User inserts their Access Card into the card reader and enters a valid PIN.

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 file’s origin can be verified by using the creator’s public key, which can be obtained from the file's author.

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 a Microsoft® Window's 7 based operating systems using the using a drive configured the NTFS file system.

In order to perform the installation of DSO, the user must be an administrator of the workstation. The installation requires the install program to install components to the operating system that are necessary for correct operation. The install program will also create the correct user groups in the system.

DSO Components

- Axalto USB v.3 or other supported USB Smart Card Reader shipped with system.
- 10 DSI/Ponemah Initialized Smart Cards

Installation

Hardware Installation

If the Data Security Option is to be installed, the supported Card Reader can be connected prior to installation of the software as follows:

USB Card Reader

For the supported USB Card Readers, follow the instructions below before running the CD-ROM Installation:

- Connect the USB connector to one of the Computers USB connections.
- When the **Found New Hardware Wizard** starts, click on the **Cancel** button.

Software Installation

1. Insert the CD-ROM into the CD-ROM drive.
2. If the Ponemah Setup program is automatically displayed, go to Step 5.
3. If the Ponemah Setup program is not automatically displayed, from the Windows Start button, select **Run**.
4. Browse to the location of the User CD drive and double click on **Install.exe**. Now click on the **OK** button in the Run dialog box to bring up the Life Science Suite Setup program.

5. To install the Data Security components, click on **Install Data Security Option** (for systems that have the Data Security Option enabled in the license file) in the Life Science Suite Setup program.
6. At the **Welcome** menu, click on the **Next** button.
7. In the **License Agreement** menu, click on the **Next** button.
8. Click on the **Install** button in the **Ready to Install Program** menu. The install program will begin to install the Data Security components.
9. In the **InstallShield Wizard Completed** menu, click on the **Finish** button when installation is complete.
10. If the Data Security Option was installed, the system must be re-booted.

To install the P3 Mail Reader option, click on **Install P3 Mail Reader** and follow the prompts.

After the installation is complete, a Ponemah Administrator must secure the directories to where data will be written, secure the Ponemah system, and grant Users authorization to the system.

Making a System Secure

Overview

On completing the above installation, the Ponemah system is operational but it is not considered a secured system. After installing the Ponemah software, including the Data Security Option, 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 an authorized Access Card, valid PIN and have 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.

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: Access Card initialization.

Step 9.) Ponemah Administrator: Setup Access Levels.

Step 10.) Ponemah Administrator: Grant Users Access to Ponemah.

Step 11.) Ponemah Administrator: Set System Security Preferences.

Step 12.) Ponemah User: Card Initialization.

Setting Up Accounts and Securing Window Directories

Step 1 - Setting User's Windows Accounts (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.

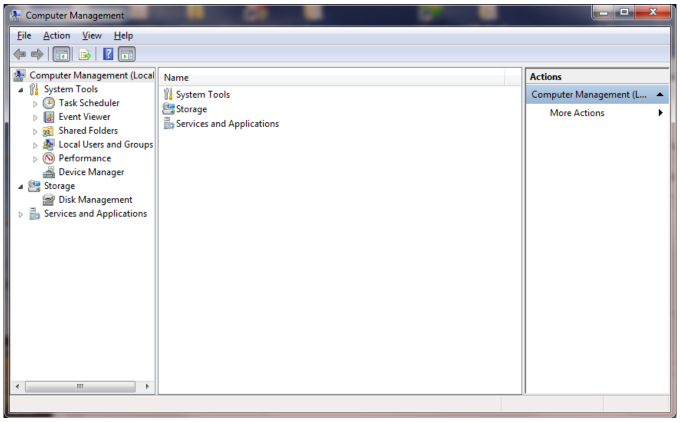
The following installation instructions illustrate an install using Windows 7 SP1. Create Windows accounts for users of Ponemah. These accounts must be members of the **P3_Users** group. A single user's account may be used to log on to Ponemah or an account may be created for each user.

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.

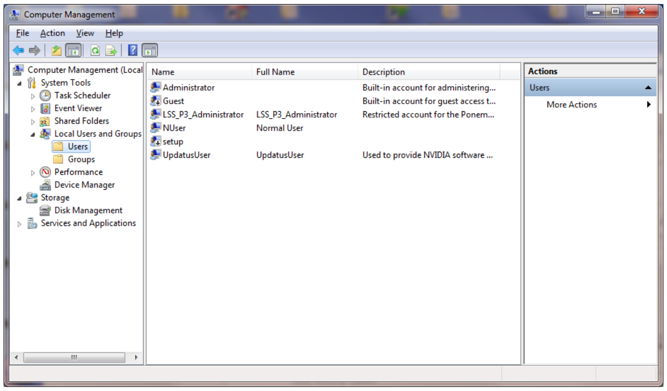
Right click on **Computer** and select **Manage**.

A dialog similar to the one below will appear:



Computer Management (Local)

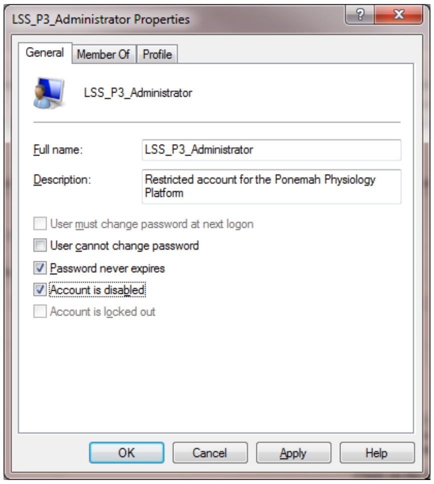
Select the **Users** folder underneath **Local Users and Groups**. The dialog will look similar to the one below:



Name	Full Name	Description
Administrator		Built-in account for administering...
Guest		Built-in account for guest access t...
LSS_P3_Administrator	LSS_P3_Administrator	Restricted account for the Ponem...
NUser	Normal User	
setup		
UpdatusUser	UpdatusUser	Used to provide NVIDIA software ...

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

Full name: LSS_P3_Administrator

Description: Restricted account for the Ponemah Physiology Platform

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

☑ Account is disabled

□ Account is locked out

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.

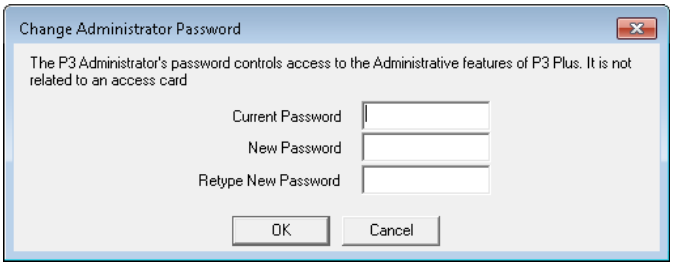
Next time the computer is restarted, this setting will take place.

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

The P3 Administrator's password controls access to the Administrative features of P3 Plus. It is not related to an access card

Current Password
New Password
Retype New Password

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.

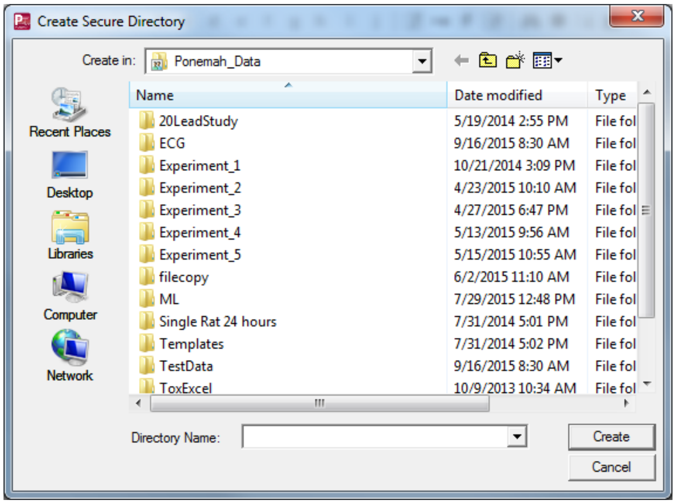
Creation and securing of directories is listed in the application log.

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.

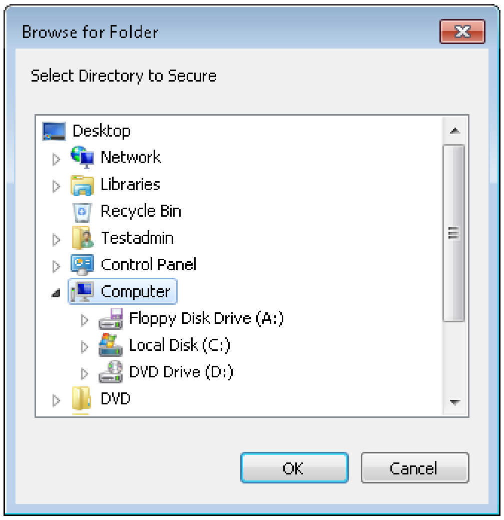


Create in: Ponemah_Data

Name	Date modified	Type
20LeadStudy	5/19/2014 2:55 PM	File fol
ECG	9/16/2015 8:30 AM	File fol
Experiment_1	10/21/2014 3:09 PM	File fol
Experiment_2	4/23/2015 10:10 AM	File fol
Experiment_3	4/27/2015 6:47 PM	File fol
Experiment_4	5/13/2015 9:56 AM	File fol
Experiment_5	5/15/2015 10:55 AM	File fol
filecopy	6/2/2015 11:10 AM	File fol
ML	7/29/2015 12:48 PM	File fol
Single Rat 24 hours	7/31/2014 5:01 PM	File fol
Templates	7/31/2014 5:02 PM	File fol
TestData	9/16/2015 8:30 AM	File fol
ToxExcel	10/9/2013 10:34 AM	File fol

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.

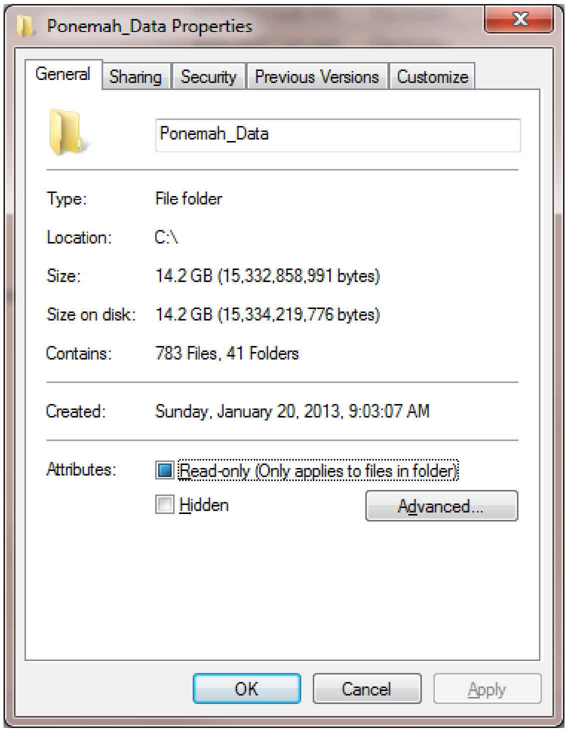


Securing Existing Directory Manually

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. For Windows 7, select Properties by right clicking the mouse on the appropriate folder.

The directory **Properties** window will be displayed:



Ponemah_Data

Type: File folder

Location: C:\

Size: 14.2 GB (15,332,858,991 bytes)

Size on disk: 14.2 GB (15,334,219,776 bytes)

Contains: 783 Files, 41 Folders

Created: Sunday, January 20, 2013, 9:03:07 AM

Attributes: ■ Read-only (Only applies to files in folder)

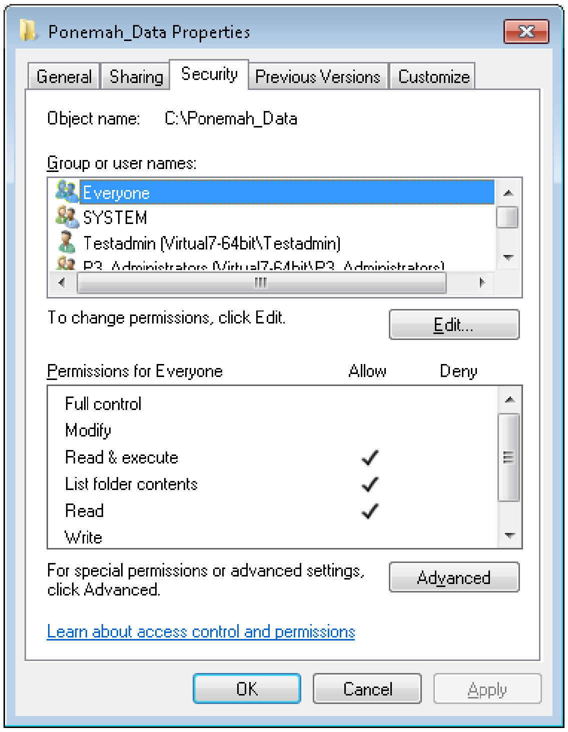
□ Hidden

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:



Object name: C:\Ponemah_Data

Group or user names:

- Everyone
- SYSTEM
- Testadmin (Virtual7-64bit\Testadmin)
- P3_Administrators (Virtual7-64bit\P3_Administrators)

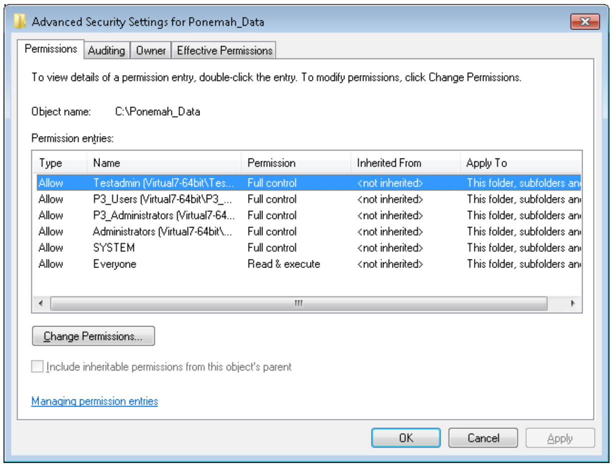
To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

Ponemah_Data Properties - Security Tab

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



To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: C:\Ponemah_Data

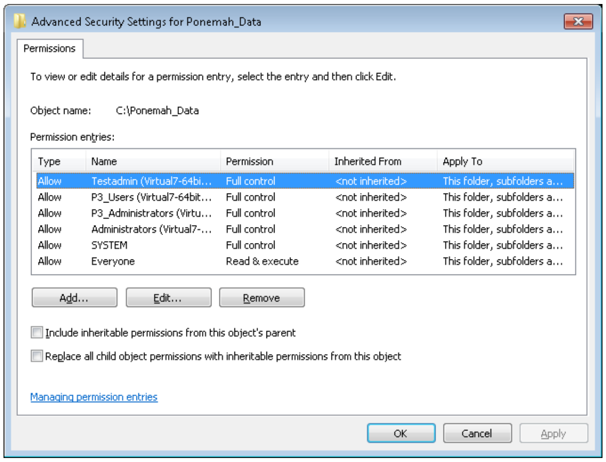
Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Testadmin (Virtual7-64bit\Tes...	Full control	<not inherited>	This folder, subfolders an
Allow	P3_Users (Virtual7-64bit\P3_...	Full control	<not inherited>	This folder, subfolders an
Allow	P3_Administrators (Virtual7-64...	Full control	<not inherited>	This folder, subfolders an
Allow	Administrators (Virtual7-64bit\...	Full control	<not inherited>	This folder, subfolders an
Allow	SYSTEM	Full control	<not inherited>	This folder, subfolders an
Allow	Everyone	Read & execute	<not inherited>	This folder, subfolders an

□ Include inheritable permissions from this object's parent

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.



To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Ponemah_Data

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Testadmin (Virtual7-64bi...	Full control	<not inherited>	This folder, subfolders a...
Allow	P3_Users (Virtual7-64bit...	Full control	<not inherited>	This folder, subfolders a...
Allow	P3_Administrators (Virtu...	Full control	<not inherited>	This folder, subfolders a...
Allow	Administrators (Virtual7-...	Full control	<not inherited>	This folder, subfolders a...
Allow	SYSTEM	Full control	<not inherited>	This folder, subfolders a...
Allow	Everyone	Read & execute	<not inherited>	This folder, subfolders a...

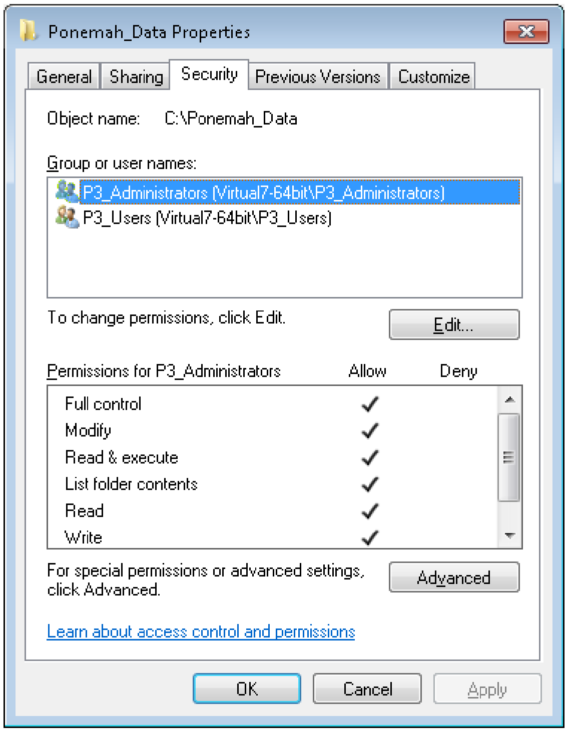
□ Include inheritable permissions from this object's parent

□ Replace all child object permissions with inheritable permissions from this object

Managing permission entries

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.



Object name: C:\Ponemah_Data

Group or user names:

- P3_Administrators (Virtual7-64bit\P3_Administrators)
- P3_Users (Virtual7-64bit\P3_Users)

To change permissions, click Edit.

Permissions for P3_Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

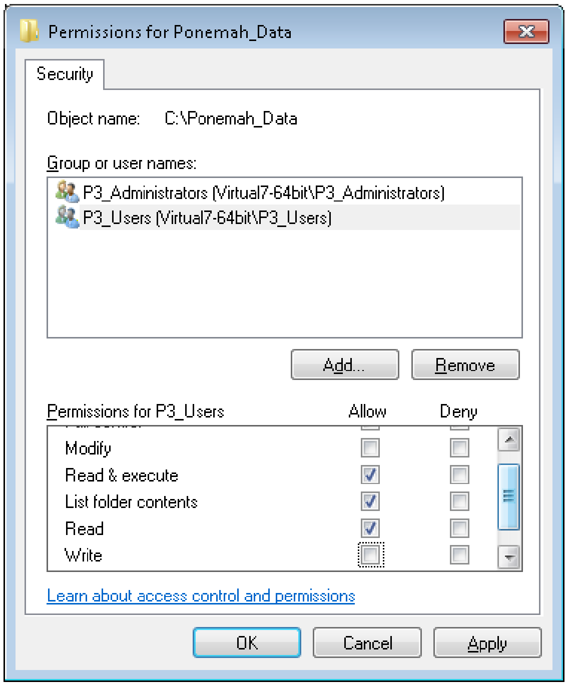
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

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**.



Permissions for Ponemah_Data

Security

Object name: C:\Ponemah_Data

Group or user names:

- P3_Administrators (Virtual7-64bit\P3_Administrators)
- P3_Users (Virtual7-64bit\P3_Users)

Permissions for P3_Users	Allow	Deny
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	□	□

Learn about access control and permissions

P3_User Permissions

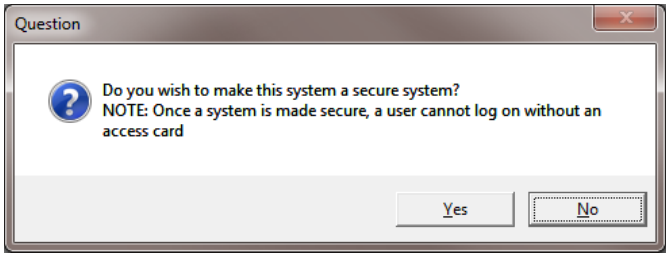
Click on the **OK** button.

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.



Question

Do you wish to make this system a secure system?
NOTE: Once a system is made secure, a user cannot log on without an access card

Secure System Dialog

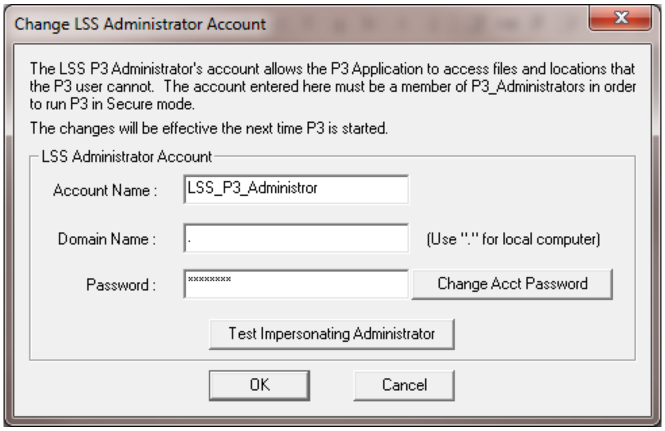
Once a system is secured, it cannot be accessed without a card reader, the software license file with the security option enabled, and a valid Access Card and PIN. The system can be unsecured by the Ponemah Administrator. See Appendix D "Unsecuring System" for details.

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

If P3 data is going to be copied using Data Manager or if P3 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
X
LSS Administrator Account
Change Acct Password
Test Impersonating Administrator
OK
Cancel

The LSS P3 Administrator's account allows the P3 Application to access files and locations that the P3 user cannot. The account entered here must be a member of P3_Administrators in order to run P3 in Secure mode.

The changes will be effective the next time P3 is started.

Account Name : LSS_P3_Administror

Domain Name : . (Use "." for local computer)

Password : *********

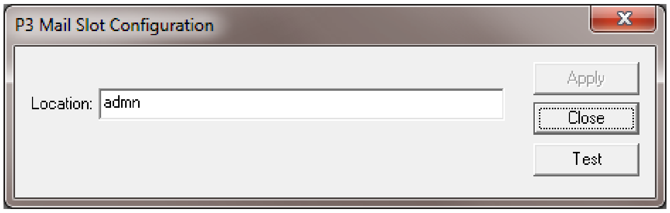
Change LSS Administrator Account Dialog

- **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.
    - **Enter Accounts Old Password** - This edit box requires the user to input the current password for the Administrator's account.
    - **Enter Accounts New Password** - This edit box allows the Ponemah Administrator to enter a new Password.
    - **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: ??? Failure – check service

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



Location: admn

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

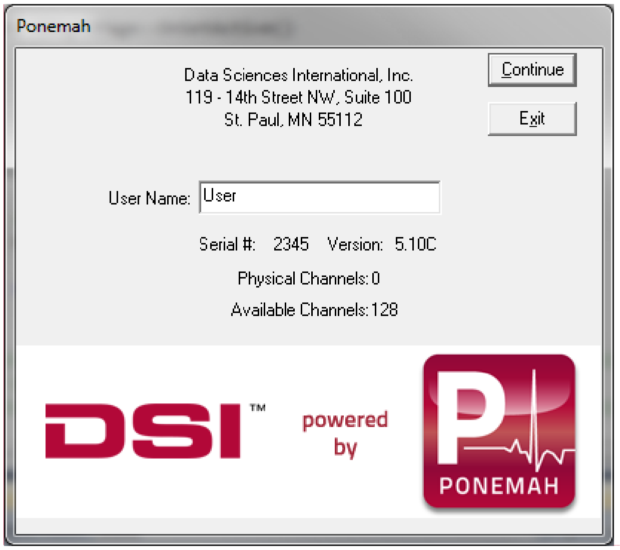
To configure the mail slot notification on a Ponemah system, set the **Location** to the current domain/workgroup in the **P3 Mail Slot Configuration** dialog and click on the **Apply** button.

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 - Access Card Initialization (Ponemah Administrator)

Insert an un-initialized (unassigned Access Card that has no private keys created on the card) in the Card Reader. The **Ponemah Physiology Platform** dialog will appear prompting for the Access Card's PIN to be entered. Note: All cards shipped from DSI/Ponemah have a default PIN of "00000000" (i.e. eight zeros). The default PIN may be changed in the P3 Admin application.



Data Sciences International, Inc.
119 - 14th Street NW, Suite 100
St. Paul, MN 55112

User Name: User

Serial #: 2345 Version: 5.10C

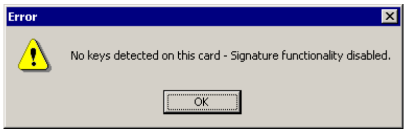
Physical Channels: 0

Available Channels: 128

Commented [KJJ1]: New screen capture

Ponemah Physiology Platform Dialog

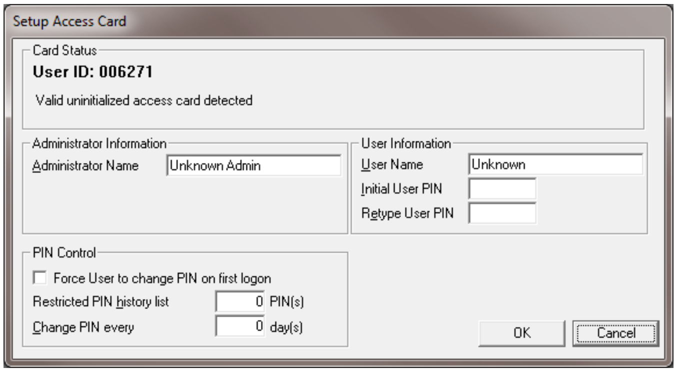
If the Access Card is not initialized with keys, the system will display the following message (This message is expected and will continue to appear until the individual that the card is assigned to create keys on the access card. Click on the **OK** button):



No keys detected on this card - Signature functionality disabled.

No Keys Message

From the **Tools** Menu in the Ponemah Admin application, select **Access Card Setup**. The following dialog will be displayed:



Setup Access Card

Card Status

User ID: 006271

Valid uninitialized access card detected

Administrator Information

Administrator Name: Unknown Admin

User Information

User Name: Unknown

Initial User PIN:

Retype User PIN:

PIN Control

☐ Force User to change PIN on first logon

Restricted PIN history list: 0 PIN(s)

Change PIN every: 0 day(s)

Setup Access Card Dialog

NOTE: When assigning an Access Card to a User, use an un-initialized Access Card (card with no private keys created).

In the **Setup Access Card** dialog, the Access Card's User ID will appear; this number will match the User ID stamped on the card. If no private keys have been created for the card, the dialog will display the message, "Valid un-initialized access card detected". In the **Setup Access Card** dialog, the Ponemah Administrator sets up the following on the Access Card:

- **Administrator Name** - the Ponemah Administrator who is responsible for assigning the Access Card.
- **User Name** - the name of the User assigned to the Access Card. The User Name is also used to represent the electronic signature in human-readable form; the User Name will be appear in .LOG files, printouts, and with electronic signature information displayed in the **Verify Files** dialog.

  NOTE: For GLP compliance, the User Name should be entered according to how the individual signs their name. For example, if the User uses their middle initial, then their name should be entered as follows: "John D. Doe".
- **Initial User PIN** - this is the PIN that is initially assigned to the Access Card so that the User is able to gain access to the Ponemah system for the first time. It is recommended that upon first logon to the system, the User should change the PIN to be unique and personalized.

  NOTE: The PIN must be 8 characters.
- **PIN Control** - this section allows the Ponemah Administrator to set up further security controls on the Access Card.
  - **Force User to change Password on first logon** - enabling this feature will force the User to change the PIN, originally assigned by the Ponemah Administrator, after their first logon to the system. After entering the Ponemah application, the **Change PIN** dialog (see **Change PIN**) will appear forcing the User to change their PIN.
  - **Restricted PIN history list** - This feature may be used to prevent PIN re-use. If a number other than 0 is entered here, the User's old PINs will be preserved on the Access Card and the User will

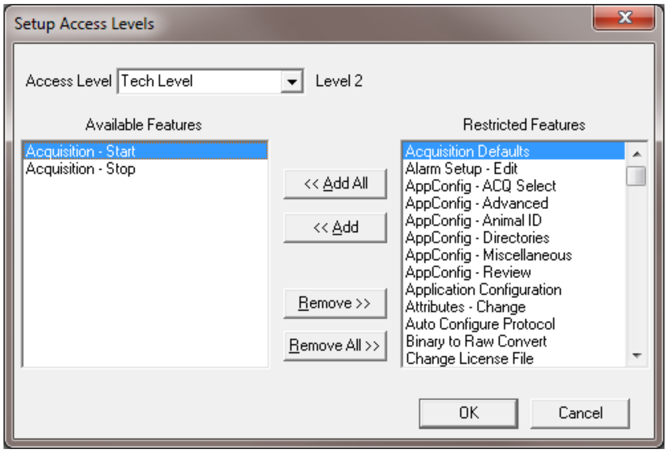
be prevented from re-using any of these PINs. The length of the list depends on the number entered, the maximum being 10.

- **Change PIN every x days** - this option forces the User to periodically change their PIN; the time period is defined by the Ponemah Administrator; the maximum number of days that can defined is 999.

Once the User has created private keys on the Access Card, the Ponemah Administrator Information and User Information in the **Setup Access Card** dialog cannot be changed; therefore, Access Cards cannot be reassigned to new Users.

Step 9 - 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.



Access Level: Tech Level Level 2

Available Features:
Acquisition - Start
Acquisition - Stop

Restricted Features:
Acquisition Defaults
Alarm Setup - Edit
AppConfig - ACQ Select
AppConfig - Advanced
AppConfig - Animal ID
AppConfig - Directories
AppConfig - Miscellaneous
AppConfig - Review
Application Configuration
Attributes - Change
Auto Configure Protocol
Binary to Raw Convert
Change License File

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.

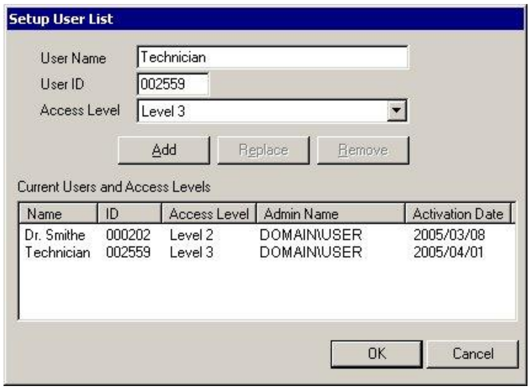
Remove All>>/Remove>> - These buttons allow features to be moved from the Available Features list to the Restricted Features list either by removing all features or by removing each selected feature, respectively.

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

Step 10 - 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.



User Name: Technician
User ID: 002559
Access Level: Level 3

Current Users and Access Levels

Name	ID	Access Level	Admin Name	Activation Date
Dr. Smithe	000202	Level 2	DOMAIN\USER	2005/03/08
Technician	002559	Level 3	DOMAIN\USER	2005/04/01

Setup User List Dialog

User Name - This edit box allows the Ponemah Administrator to type in the name of the User who is being granted access to the system. This name is used only for ease of identifying the User; it will not be used to represent the User's electronic signature.

User ID - This edit box allows the Ponemah Administrator to type in the identification number assigned to the User's Access Card. This is the number that the system will recognize when verifying that the User has authority to Access the system.

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.

Replace - 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.

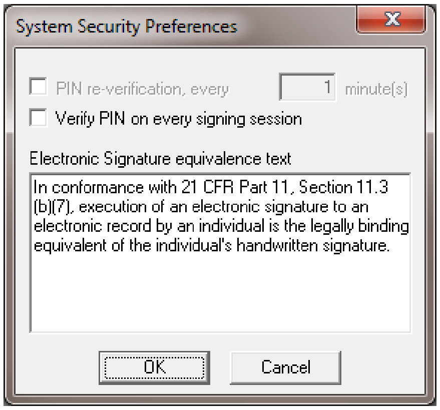
> **NOTE: If the User's Access Card is lost, stolen, or corrupted, the Ponemah Administrator can delete the User (delete the User's Access Card) from all applicable systems. Deleting the User's Access Card will prevent an individual from gaining access to the system using the Access Card.**

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 11 - 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

□ PIN re-verification, every 1 minute(s)

□ Verify PIN on every signing session

Electronic Signature equivalence text

In conformance with 21 CFR Part 11, Section 11.3 (b)(7), execution of an electronic signature to an electronic record by an individual is the legally binding equivalent of the individual's handwritten signature.

System Security Preferences Dialog

- **PIN verification every x minutes** - Enabling this check box will force Users to re-enter their PINs every x minutes.
- **Verify PIN on every signing session** - Enabling this check box will force Users to re-enter their PIN upon every execution of an electronic signature (to a group of files). If not selected, the User will be asked for a PIN 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 PIN (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 12 - Card Initialization (Ponemah User)

When the User receives the Access Card from the Ponemah Administrator, the card should be set up with the User's name and a PIN (this initial PIN is set up by the Ponemah Administrator). Prior to using the Access Card to electronically sign data, the User must store a public/private key pair to the card. When the Ponemah Administrator inserts an un-initialized card in the Ponemah system, the Administrator will NOT be prompted to create keys, only a User can create keys. If an Administrator is also a User, it is recommended that the Administrator use two separate login ID's.

The following options are available to create public/private key pairs:

1. The user logs on to a Certifying Authority's website, managed by a trusted source such as VeriSign®, and obtains a digital ID after entering personal information and after the trusted source completes its verification process.
2. Allow the Ponemah program to generate the keys.

   If the user chooses to have the Ponemah program generate the keys, the program will detect a card without keys on it, and prompt the user to generate with the Ponemah system.

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 an Access Card to each User 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 on the User's Access Card 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 an Access Card is in the card reader.
- Verify that a valid PIN for the Access Card has been entered into the startup dialog.
- Verify that the Access Card's User ID is on the system's User List.
- Verify the User's Access Level on the system.

Defining Controlled Access to the System

Once the Ponemah User has inserted their Access Card into the Card Reader and entered a valid PIN, the User gains control over the Ponemah System. The User is granted continuous control over the system until the User removes their Access Card from the card reader. Upon removal of the Access Card, the User, nor any other individual, will have access to the system. In order to regain control, the system will require the User to insert their Access Card into the card reader and enter a valid PIN.

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 PIN for the Access Card. The system will not grant the User the ability to perform any operations in the system until the User has appropriately verified control.

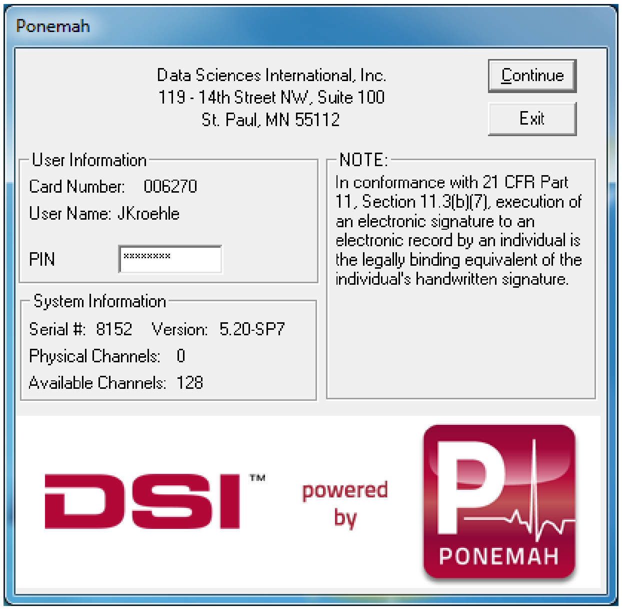
While the Ponemah application is open, the system will allow multiple Users to log on and log off the system. The User who wants to perform any operations within the Ponemah application must use their Access Card and PIN appropriately.

If an Access Card is not present in the system, 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 (no Access Card present in the Card Reader), 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 be required to have an authorized Access Card, valid PIN 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, insert the Access Card into the card reader and start the Ponemah application. Upon startup, the following dialog will appear prompting the User to enter a valid PIN for the Access Card:



Data Sciences International, Inc.
119 - 14th Street NW, Suite 100
St. Paul, MN 55112

User Information
Card Number: 006270
User Name: JKroehle
PIN ********

System Information
Serial #: 8152 Version: 5.20-SP7
Physical Channels: 0
Available Channels: 128

NOTE:
In conformance with 21 CFR Part 11, Section 11.3(b)(7), execution of an electronic signature to an electronic record by an individual is the legally binding equivalent of the individual's handwritten signature.

Ponemah Physiology Platform Secure Login Dialog

Upon entering a valid PIN for the Access Card, 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 remove their Access Card from the card reader.

If the User does not use all the correct components required to access the system, the following error messages will appear:

- If an Access Card is not inserted into the Card Reader, then the System will display the following warning message: "No Access Card available. Please insert an Access Card and select OK, or hit Cancel to Exit."
- If a User is not on the system's User List, then the system will display the following warning message when an un-authorized User tries to gain access to the system: "The user is not permitted to use this system. Please remove the Access Card and contact your system administrator."

- To prevent un-authorized Users from gaining access to the Ponemah, an Access Card will be rendered useless if five consecutive invalid attempts to enter a PIN occur (this security control is not optional). If the User is prompted to enter a valid PIN for each signing, the Access Card will be rendered useless if five consecutive invalid attempts to enter a PIN occur.
- If the Access Card is removed, the System will display the following warning message: "No access card present or card was inappropriately removed - Please insert/reinsert card." Upon re-inserting the Access Card, the system will require the Ponemah User to enter their PIN.

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. .SIG files can only be created using an Access Card and PIN; therefore, an electronic signature cannot be falsified by any other means. Electronic signatures are verified for their integrity and can be viewed in human readable form using the **Verify** utility.

Executing an electronic signature for the first time requires the use of two components: An Access Card and PIN. The first signing is executed when the User logs onto the system. During a continuous session, executing electronic signatures only requires the Access Card. However, the Ponemah Administrator can force Users to use both their Access Card and PIN in order to execute each electronic signature during a continuous session.

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, .XLSB, .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.

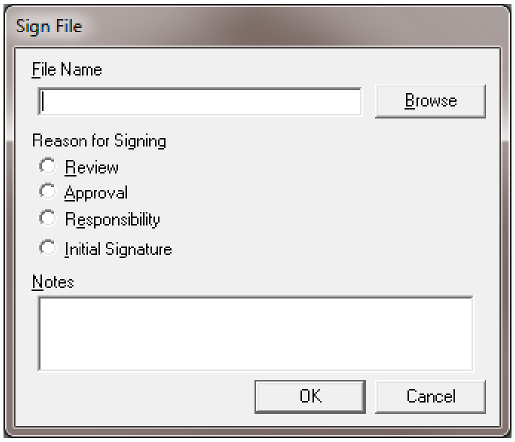
- Using Windows Task Manager (<Ctrl><Alt><Del>) to shut down the Ponemah application.
- If the system unexpectedly terminates (system crash) during use of the Ponemah application, opened files will not be signed.

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.

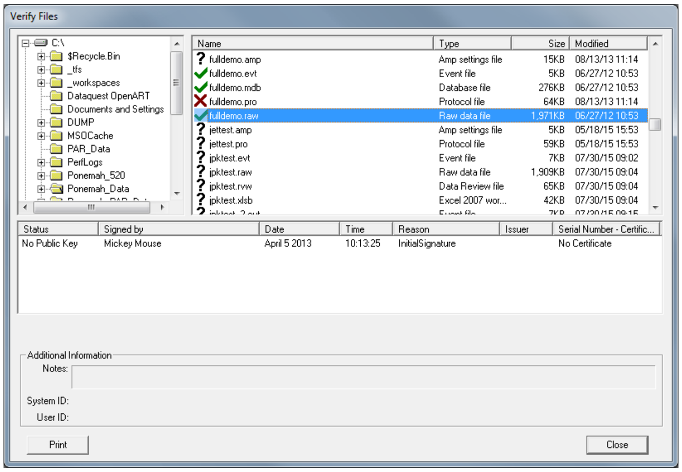
Note: It is recommended that the User use Data Manager when copying or moving files to new locations. The Data Manager utility maintains the integrity of the link between electronic records and electronic signatures. Upon moving or copying of files, the User should verify that the integrity of the electronic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



	Name	Type	Size	Modified
?	fulldemo.amp	Amp settings file	15KB	08/13/13 11:14
✓	fulldemo.evt	Event file	5KB	06/27/12 10:53
✓	fulldemo.mdb	Database file	276KB	06/27/12 10:53
✗	fulldemo.pro	Protocol file	64KB	08/13/13 11:14
✓	fulldemo.raw	Raw data file	1,971KB	06/27/12 10:53
?	jettest.amp	Amp settings file	5KB	05/18/15 15:53
?	jettest.pro	Protocol file	59KB	05/18/15 15:53
?	jpktest.evt	Event file	7KB	07/30/15 09:02
?	jpktest.raw	Raw data file	1,909KB	07/30/15 09:04
?	jpktest.rvw	Data Review file	65KB	07/30/15 09:04
?	jpktest.xlsb	Excel 2007 wor...	42KB	07/30/15 09:04

Status	Signed by	Date	Time	Reason	Issuer	Serial Number - Certific...
No Public Key	Mickey Mouse	April 5 2013	10:13:25	InitialSignature		No Certificate

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:

Commented [KJJ2]: Need something about Review files and mark sections

- ***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):
  - Electronic records that were originally created on a non-secured system will not be signed.
  - 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.
  - 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.
  - 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).
  - 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 and 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.

Status - Indicates the validity of the electronic signature. If a Public Key was found for the electronic signature, then **Verified** will be displayed for the status of the electronic signature; otherwise, **No Public Key** will be displayed.

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).

Issuer - the information listed in this column is dependent upon thee different scenarios that deal with how keys were created for the Access Card. The Issuer represents the following:

- If keys were created using VeriSign, then VeriSign will be listed as the "Issuer".
- If a public key was imported on the system to verify the User's electronic signature, then the name that the Ponemah Administrator entered in the **Key Identifier** edit field in the **Import Public Key** dialog (see Import Public Key), will be displayed.
- If keys were created for Access Card by the same Ponemah system that is being used to verify the electronic signature, then the User Name will be displayed (When keys are created on a Ponemah System, the Key Identifier is automatically set to the User Name).

Serial Number - Certificate - Indicates the serial number of the certificate if a certificate was imported.

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.

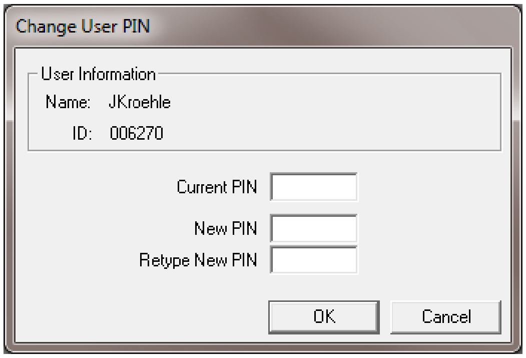
User ID - Indicates which Access Card was used to generate the electronic signature.

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

Change User PIN

The **Change User PIN** dialog allows the User to change the PIN associated with their Access Card.

To open this dialog, start the Ponemah application and select **Change User PIN** from the **Tools** menu.


Change User PIN

User Information

Name: JKroehle

ID: 006270

Change User PIN Dialog

The user must enter their current PIN and then enter their new PIN. To accept their new PIN, the User must click on the **OK** button.

The Ponemah Administrator may set up additional security controls on the User's Access Card. The Administrator has the option to force the User to periodically change their PIN and prevent PIN re-usage. The **Change User PIN** dialog will automatically appear upon the Administrator's scheduled time period when the User logs onto the system, forcing the User to change their PIN. Each time the User sets up a PIN, the Access Card maintains a list of the previously used PINs. Upon setting up a new PIN, the system will not allow the User to re-use any of the PINs that are currently on the list. The User will not be able to perform any functions within the Ponemah application until their PIN has been correctly changed.

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 on the Access Card, and the Access Level that has been assigned to the Access Card.

Using Public/Private Keys

The Data Security Option employs public/private key pair technology. These keys are created when the user authorizes creation of the keys on their Access Card (see Installation - Step 12 - Card Initialization (Ponemah User)) either using the Ponemah application or VeriSign to create the keys.

Public and private keys are used to sign Ponemah files. These keys are not identical, but are mathematically related. The user retains the private (retained solely on the user's Access Card) and uses the private key to sign the electronic record information when they execute an electronic signature. The user then distributes the public key to anyone (or any system) they choose. The public key is used to verify the signature of the electronic record information, and therefore, verify the identity of the individual who signed the Ponemah files.

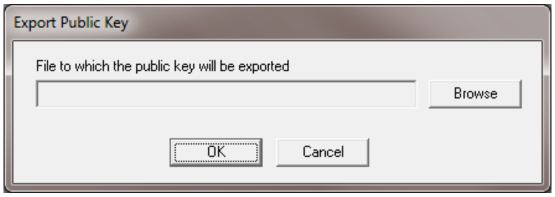
In order to permit Ponemah to confirm the identity of the signer, the user must make their public key available on the Ponemah system. When the user creates keys on a Ponemah system, the public key is automatically retained on system where the keys were created. However, if signatures need to be verified on a system where the user did not create their keys, then the user needs to make their public key available on that system. To distribute a public key, the user must export their public key in the Ponemah application (see Export Public Key). Upon export, the P3 Administrator can import the public key in the P3 Admin application, and therefore, make it available on the system to verify signatures (see Import Public Key). Import of a user's public key only needs to be performed once on a system.

When the user verifies a signature in the Verify dialog, the Status column will indicate the validity of the electronic signature. If a public key was found for the electronic signature, then Verified will be displayed for the status of the electronic signature; otherwise, No Public Key will be displayed.

Export Public Key

The **Export Public Key** allows a User to export their public key so that it can be sent to other Users. The public key can then be imported so that it could be used to verify files. A user can export their public key using the **Export Public Key** function, regardless if the Ponemah application or VeriSign created the user's keys. However, if the user used VeriSign to create keys, the user has the option of distributing their public key through Certificates through the Microsoft Windows operating system (For more information, refer to section Associating Digital ID With E-Mail Account).

Select **Export Public Key** from the **Tools** menu in the Ponemah application. The following dialog will be displayed:



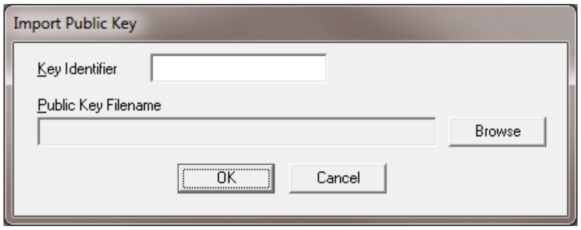
Export Public Key Dialog

Click on the **Browse** button and navigate to the location where the key will be exported.

Import Public Key

Importing public keys to verify signing of files can be performed in the Ponemah Admin application. Importing public keys on a system will need to be performed if the Access Card's public/private keys (the Access Card used to sign the electronic files) were created on another Ponemah system or if the public/private keys were created by a third-party source, such as VeriSign. Upon importing public keys, the User will be able to verify integrity of the files in the **Verify Files** dialog (Ponemah application).

Select **Import Public Key** from the **Tools** menu in the Ponemah Admin application. The following **Import Public Key** dialog will be displayed:

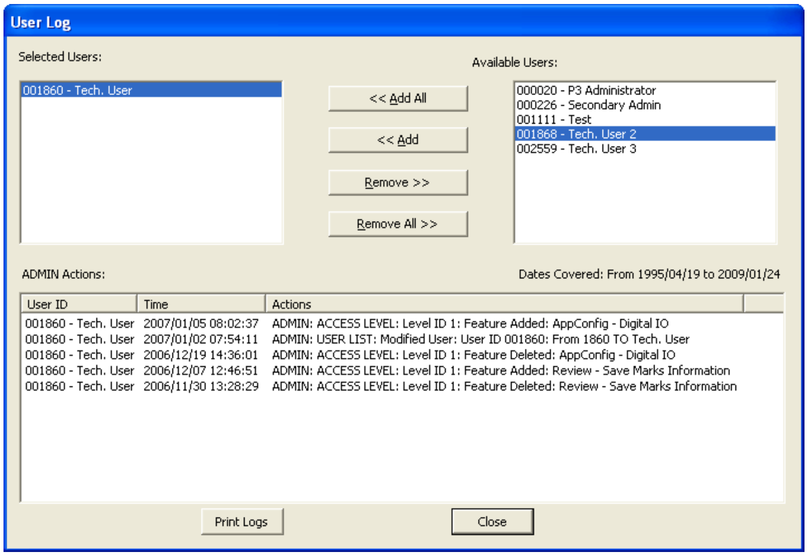


Import Public Key Dialog

Enter a name in the **Key Identifier** edit field; the Key Identifier is used to represent the User for who the public key is being imported to verify the electronic signature. The **Key Identifier** will be displayed in the **Issuer** column of the **Verify Files** dialog when a match is found with an imported key. If the Key Identifier already exists, the Ponemah Administrator will be prompted if they want it overwritten. Click on the **Browse** button and navigate to the location of the Public Key that needs to be imported.

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.



Selected Users:

- 001860 - Tech. User

Available Users:

- 000020 - P3 Administrator
- 000226 - Secondary Admin
- 001111 - Test
- 001868 - Tech. User 2
- 002559 - Tech. User 3

ADMIN Actions:

Dates Covered: From 1995/04/19 to 2009/01/24

User ID	Time	Actions
001860 - Tech. User	2007/01/05 08:02:37	ADMIN: ACCESS LEVEL: Level ID 1: Feature Added: AppConfig - Digital IO
001860 - Tech. User	2007/01/02 07:54:11	ADMIN: USER LIST: Modified User: User ID 001860: From 1860 TO Tech. User
001860 - Tech. User	2006/12/19 14:36:01	ADMIN: ACCESS LEVEL: Level ID 1: Feature Deleted: AppConfig - Digital IO
001860 - Tech. User	2006/12/07 12:46:51	ADMIN: ACCESS LEVEL: Level ID 1: Feature Added: Review - Save Marks Information
001860 - Tech. User	2006/11/30 13:28:29	ADMIN: ACCESS LEVEL: Level ID 1: Feature Deleted: Review - Save Marks Information

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.

Reset PIN

To Reset the PIN of a deactivated card, with the card removed from the card reader start the Ponemah Admin application. Insert the deactivated card and ignore the log on dialog. Select Reset PIN and the user will be asked are you sure?

Responding Yes will reset that cards PIN to **AAAAAAAA.** At this time the user can enter AAAAAAAA into the login dialog and it will be accepted.

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 unauthorized Access Card or invalid PIN 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: ILLEGAL CARD :/ILLEGAL LOGIN", the User ID, and the User Name of the card 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:

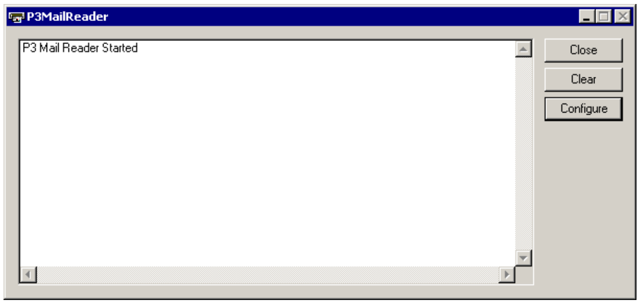
Commented [KJJ3]: Update

- 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

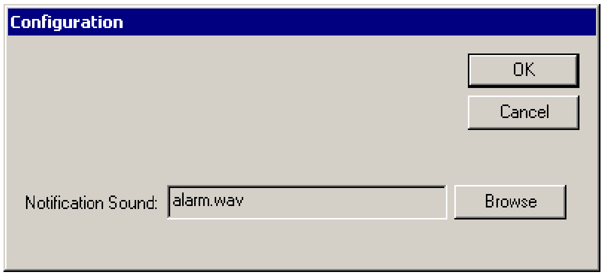
The User has the option of setting-up a .WAV file that is played on the computer when an illegal logon attempt is performed.



P3 Mail Reader Started

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.



Notification Sound: alarm.wav

Configuration Dialog

Obtaining a Digital ID Through VeriSign

Overview

Digital IDs can be used to verify information being transferred from person to person is valid data.

Steps to Obtain Personal Digital ID

The steps listed below run the User through the process of obtaining a Digital ID through the VeriSign web site. The Card Reader must be installed and an Access Card that does not have a key pair must be in the card reader.

NOTE: **The information listed is subject to change. Data Sciences International does not control or cannot be held responsible for obsolete information.**

1) Log on to http://www.VeriSign.com.
2) Select **PRODUCTS/SERVICES** from the menu in the upper portion of the window.
3) Select **Digital IDs for Secure E-mail** listed under **Products and services by name** from the **Security Products & Services** drop down list box and click on the double arrows to the right.
4) Read through the information and select the **BUY NOW** button located near the top of the page.
5) Read through the information and select the **ENROLL NOW** button located near the bottom of the page. If a Security Alert message is posted, click on the **OK** button.
6) Read and fill out the application.

NOTE: It is recommended to use a unique name when filling out the application for VeriSign. To view the unique names associated with each certificate already on a system, start the Outlook application, select **Options** from the **Tools** menu, click on the **Security** tab, click on the **Import/Export** button, select **Export your Digital ID to a file**, and then click on the **Select** button.

7) Select **Schlumberger Cryptograph Service Provider** as the **Cryptographic Service Provider Name**.

NOTE: **It is suggested to set the Additional Security for Your Private Key to a High setting.**

8) Once you click on the **Accept** button, a message will come up confirming your e-mail address. If it is correct, click on the **OK** button.

9) Receive the e-mail from VeriSign and read it.

10) Copy the Digital ID PIN, go to VeriSign's secure Digital ID Center, paste the Digital ID PIN, and click on the **Submit** button.

11) Click on the **INSTALL** button.

Your personal digital ID has been installed.

Associating Digital ID With E-Mail Account

The steps listed below run the User through the process of associating their Digital ID with their E-mail account. Microsoft Outlook will be the E-mail program that is used.

1.) Start Microsoft Outlook.

2.) Select **Options** from the **Tools** menu.

3.) Select the **Security** tab.

4.) Click on the **Change Settings** button (For Windows XP).

5.) Under the **Certificates and Algorithms** section, click on the **Choose** button for the **Signing Certificate**.

6.) Select the Digital ID that is to be used and click on the **OK** button.

7.) Click on the **OK** button on the **Change Security Settings** dialog.

8.) Click on the **OK** button on the **Options** dialog.

Once these steps have been completed, the files that you create in a secured system will have a status of **Verified** in the **Verify Files** dialog and you will have the ability to send your Digital ID with your E-mails.

Searching for Digital IDs

The steps listed below run the User through the process of searching for a Digital ID of another User.

Warning: **The information listed is subject to change. Data Sciences International does not control or cannot be held responsible for obsolete information.**

1.) Log on to http://www.VeriSign.com.

2.) Select **PRODUCTS/SERVICES** from the menu in the upper portion of the window.

3.) Select **Digital IDs for Secure E-mail** listed under **Products and services by name** from the **Security Products & Services** drop down list box and click on the double arrows to the right.

4.) Select **Search** located near the bottom of the page.

5.) Search for the Digital ID using whichever method desired.

6.) Select the name of the User.

7.) Select the **Download** button.

8.) Select **Someone Else's Digital ID for Microsoft® IE (4.0 or later)/ Outlook Express®/Microsoft® Outlook®** from the drop down list box and click on the **Download This Digital ID** button.

9.) Save the file to a known location.

10.) Navigate to the location of the file and double click on the file.

11.) Select the **Address Book** tab.

12.) Select the **Add to Address Book** button.

13.) Click on the **OK** button.

Once these steps have been completed, the files created by the owner of the digital ID will have a status of **Verified** in the **Verify Files** 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
Acquisition - Stop
Acquisition Defaults
Alarm Setup - Edit
AppConfig - ACQ Select
AppConfig - Advanced
AppConfig - Animal ID
AppConfig - Directories
AppConfig - Miscellaneous
AppConfig - Review
Application Configuration
Attributes - Change
Auto Configure Protocol
Binary to Raw Convert
Change License File
Combine RAW Files
Data Insights - Search Definition
Data Insights - Association
Data Insights - Rejection",
Data Insights - Edit Report
Data Manager-Copy
Data Manager-Delete
Data Manager-Move
Data Parser Setup
Data Reduction - Setup
Data Set Name - Setup
Derived Parameters - Select
Digital Display - Setup
Edit Digital Telemetry Configuration
Edit DSI Setup
Email Alert
Enter Online Messages
Events - Assign To Groups
Events - Label
Events - Trigger
Global Settings
Graph - Change X Axis
Graph - Change Y Axis
Graph Page - Print
Graph Page - Setup
Groups - Label
Groups - Trigger Channel
Import Raw File

Input Setup - Edit
JET Device Configuration
Jump
Logging Rate - Change
Measure - Enable
ODBC Interface
Options - Reason Codes
Overwrite - Data Files
Overwrite - Derived Files
Overwrite - Protocol Files
Printer Setup
Protocol - Open
Protocol - Save
Protocol - Save As
Protocol Header - Edit
Public Key - Export
PV Loops - Add Analysis

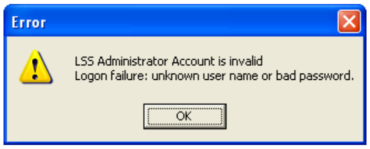
Replay - Defaults
Replay - Filename
Replay - Start
Replay - Stop
Review - Add Bad Data Sections
Review - Add Events
Review - Add Marks
Review - Add Notes
Review - Change X Axis
Review - Change Y Axis
Review - Delete Bad Data Sections
Review - Delete Events
Review - Delete Marks
Review - Delete Marks Information
Review - Delete Notes
Review - Display Options
Review - Move Bad Data Sections
Review - Move Events
Review - Move Marks
Review - Open File

Review - Open Marks Information
Review - Open Ref Information
Review - Print
Review - Print Setup
Review - Save Marks Information
Review - Save Parsed Review File
Review - Stop
Sample Rate - Setup
Save RAW Data
Scheduler - Quit
Scheduler - Setup
Scheduler - Start
Secure Directories
Select APR1
Select DSI Sources
Select Digital Telemetry Implants
Setup 7700 Amplifiers
Sign File
Study - Backup Database
Study - Change Filters
Study - Delete Study
Study - Modify
Study - New Study
Study - Overwrite Deleted Study
Study - Primary Workstation List
Study - Restore Database
Study - Run Study
Study - Save Primary Protocol
Study-Search Path
Study - Select Study
Study - Sync Entire Study
Study - Sync Study Data
Templates - Add Cycle
Templates - Analyze
Templates - Delete Cycle
Templates - Modify Binding
Templates - Modify Cycle
Time/Data Format - Setup
Video - Online Control
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.



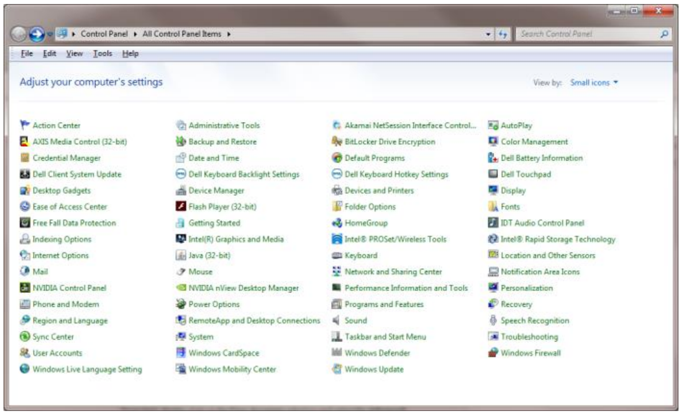
Error

LSS Administrator Account is invalid
Logon failure: unknown user name or bad password.

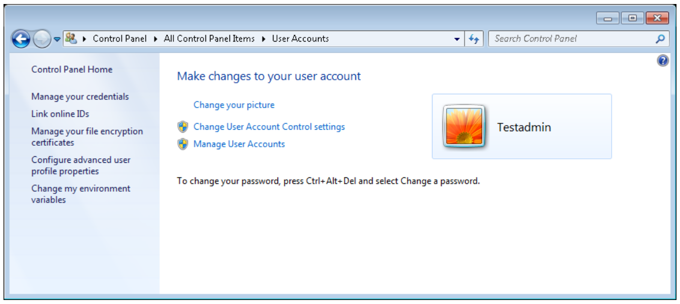
If it is not known which password has changed, run through the following steps to reset the LSS Administrator password in both Windows and Ponemah.

Correcting the Passwords

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



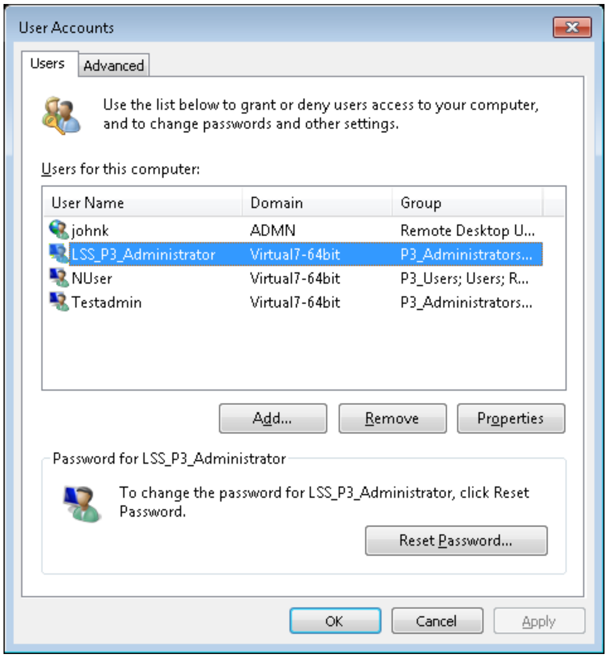
From here, click on the **User Accounts** selection.


Control Panel ▸ All Control Panel Items ▸ User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Link online IDs
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Change your picture
Change User Account Control settings
Manage User Accounts
Testadmin

Make changes to your user account

To change your password, press Ctrl+Alt+Del and select Change a password.

From here, click on **Manage User Accounts** selection.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

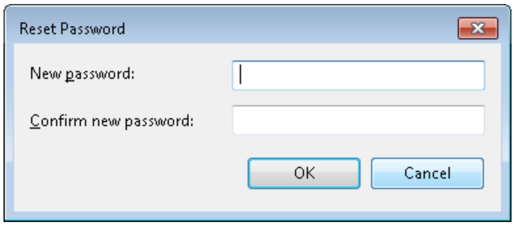
Users for this computer:

User Name	Domain	Group
johnk	ADMN	Remote Desktop U...
LSS_P3_Administrator	Virtual7-64bit	P3_Administrators...
NUser	Virtual7-64bit	P3_Users; Users; R...
Testadmin	Virtual7-64bit	P3_Administrators...

Password for LSS_P3_Administrator

To change the password for LSS_P3_Administrator, click Reset Password.

Highlight the **LSS_P3_Adminstrator** and select **Reset Password…**



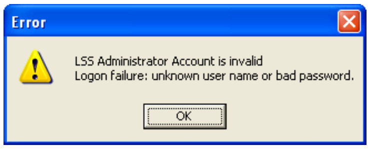
New password:

Confirm new password:

Enter a new password and then close dialog. Close the **User Accounts** dialog. Close the **Control Panel** dialog.

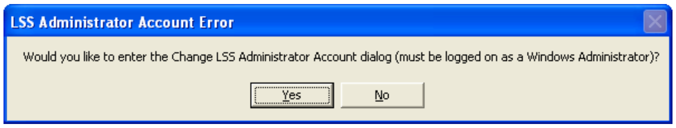
Resetting the Windows password is now complete.

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


Error

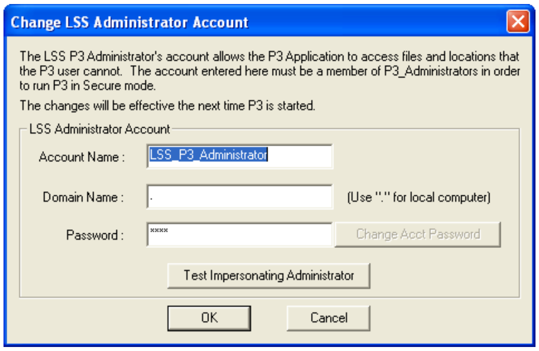
LSS Administrator Account is invalid
Logon failure: unknown user name or bad password.

Click on the **OK** button. The following dialog will appear.


LSS Administrator Account Error

Would you like to enter the Change LSS Administrator Account dialog (must be logged on as a Windows Administrator)?

Click on the **Yes** button. The following dialog will appear.


Change LSS Administrator Account

The LSS P3 Administrator's account allows the P3 Application to access files and locations that the P3 user cannot. The account entered here must be a member of P3_Administrators in order to run P3 in Secure mode.

The changes will be effective the next time P3 is started.

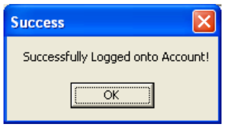
LSS Administrator Account

Account Name : LSS_P3_Administrator

Domain Name : .   (Use "." for local computer)

Password : ****

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.

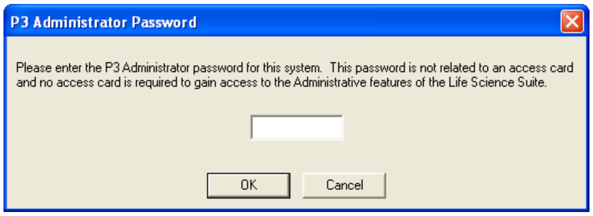

Success

Successfully Logged onto Account!

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.

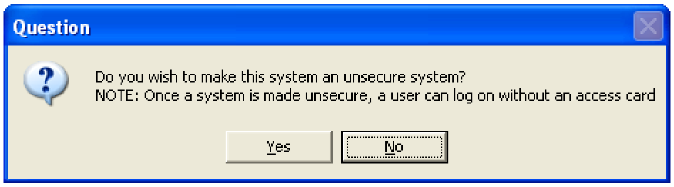


Please enter the P3 Administrator password for this system. This password is not related to an access card and no access card is required to gain access to the Administrative features of the Life Science Suite.

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.



Do you wish to make this system an unsecure system?
NOTE: Once a system is made unsecure, a user can log on without an access card

Once the **Yes** button is selected the system is now unsecured.

Product Issue Report

Product Issue Report Form

Sales Person:

Customer Name:

Company:

Address:

Phone Number:

Email Address:

Ponemah Version (including Service Pack):

Serial Number:

Priority:

Date:

Hardware:

Status of issue (check one)

[] Unreproduced [] Reproduced

[] Needs repair [] As intended

Computer hardware/software

Brand/Model:

CPU Speed:

RAM:

Operating System (including Service Pack):

Networked

[] Yes [] No

Issue:

Steps to Repeat

Feature Request

Feature Request Form

Sales Person:

Customer Name:

Company:

Address:

Phone Number:

Email Address:

Ponemah Version (including Service Pack):

Serial Number:

Priority:

Date:

Hardware:

Feature (check one)

[] Unevaluated [] Pending

[] Implement [] Already Exists

Description:

Glossary of Terms

TERM	DEFINITION
Access Card	This is a serialized Smart Card initialized by Data Sciences International. This card holds the Public/Private Key pair that establishes the identity of a user.
Access Levels	Levels defined by the Ponemah Administrator controlling the features each user has access to.
DSO	Data Security Option.
LSS_P3_Administrator	Account used by Ponemah, created during installation.
P3_Administrators	Group to which all Ponemah Administrators must belong. Membership in this group grants read/write privileges for Ponemah files.
P3_Users	Group to which all Ponemah Users must belong. Membership in this group grants read privileges for Ponemah files.
P3_Administrator	Individual with read/write access to Ponemah files and privileges to setup Users and Access Levels.
P3_User	Individual with read access to Ponemah files.
PIN	Personal Identification Number, an 8 character password, used to establish a user's identity. This is required when logging on to a Ponemah system and when signing files.
User ID	Unique number issued by Data Sciences International that is tied to an Access Card. This number is written on the Access Card and is displayed in the Ponemah login box when the card is inserted.