DSI Ponemah™

System Configuration IT Guide

OVERVIEW

This manual provides detailed computer configuration recommendations to ensure the best performance when using DSI's Implantable and Jacketed External Telemetry. In addition, it provides information on performing a complete backup of the Ponemah software platform installed on the workstation.

PN: 011404-001 Rev 12

a division of
Harvard Bioscience, Inc.

Table of Contents

PONEMAH WORKSTATION CONFIGURATION RECOMMENDATIONS

Outlined below are the recommended configuration settings for items that are known to have an impact on the function of the Ponemah acquisition workstation. These items should be checked and adjusted on the computer prior to installing and running Ponemah, as these adjustments are necessary to preserve the ability of Ponemah to control data flow during acquisition and ensure the reliability of the workstation. Failing to make these adjustments could result in lost data.

Note: Computer configurations may vary. Some of these setting may not be necessary if the particular function does not exist on the computer. Step-by-step procedures on how to configure these items are available in the Appendix.

Network Device Reference:

DSY System	Network Communication Device
PhysioTel Digital Implantable Telemetry	Communication Link Controller (CLC)
PhysioTel Legacy and PhysioTel HD Implantable Telemetry	Matrix 2.0 (MX2)
Jacketed External Telemetry (JET)	JET Bluetooth Receiver
Ambient Pressure Reference *used with pressure implants*	Ethernet to Serial Converter (E2S-1) with APR-1 OR APR-2

Windows Operating System Compatibility:

- Ponemah v5.20 Service Pack 9 and later
  - Windows® 7 SP1, 64-bit only
- Ponemah v5.3x
  - Windows® 7 SP1, or Windows® 10, 64-bit only
- Ponemah v6.50
  - Windows® 10, 64-bit only

⚠ **Caution**: *Do not install Ponemah into the Windows Program Files folder.*

FIREWALL SETTINGS

For dedicated workstations, not connected to the corporate/university network, DSI recommends disabling the Firewall.

To disable the Firewall:

1. Windows 7
   a. Select the **Windows Start menu | Control Panel | Windows Firewall.**
   b. Click on **Turn Windows Firewalls On or Off** option.
   c. Click to turn off all Firewalls.
   d. Click **OK**.
2. Windows 10
   a. Type **Windows Firewall** into the **Search Bar**.
   b. Click Windows Firewall.
   c. Click on **Turn Windows Firewalls On or Off** option.
   d. Click to turn off all Firewalls.
   e. Click **OK**.

The following Firewall settings are required to be enabled in the Firewall console for users who are required to keep their Firewall ON to allow communications with certain acquisition devices supported by Ponemah.

Note: Ponemah will attempt to open the necessary ports. However, due to certain polices, the changes may not be allowed programmatically.

Device	Settings	Comment
JET Bluetooth Receivers (JET only)	Inbound Rule UDP Port 9990 Profile: Domain/Private	Added during Ponemah installation and only used when JET is used.
JET Bluetooth Receivers (JET only)	TCP Port 21 Profile: Domain/Private	Installed as part of the operating system and FTP is needed for optimization of the JET receivers.
NTP UDP Datagram (CLC/MX2 only)	Inbound Rule UDP Port 123 Profile: Domain/Private	Added during Ponemah installation and is used only for CLCs and MX2s.
APR-2 OR **E2S-1 (APR-1) Converter (All)**	Inbound Rule UDP Port 4800 Profile: Domain/Private	Added during installation of v5.20-SP5+ and is needed for any system requiring an Ambient Pressure Reference through networking; i.e. using pressure capable implants.
Network Discovery* (UPnP-In) (All)	Inbound Rule Port TCP 2869 Profile: Domain/Private	Installed as part of the operating systems and is used to discover MX2, CLC, and E2S-1.
Network Discovery (SSDP-In) (All)	Inbound Rule Port UDP 1900 Profile: Domain/Private	Installed as part of the operating systems and is used to discover MX2, CLC, and E2S-1.
Remote Connection (e.g. Biera AeroMP or Labview)	TCP Port 6732 Profile: Domain/Private	Must be manually enabled for Remote Connection to function as expected. This default port may be modified if desired.

*It may be necessary to enable UPnP, since a UPnP-capable Operating System does not necessarily have it turned on by default. It may also be necessary to enable UPnP on the router, if not be turned on by default.

The following Firewall settings are required to be enabled if Ponemah's Study Protocol Option is being with multiple workstations (i.e. Network Study).

Rule Name	Settings	Comment
SQL Server Browser Connect	Inbound Rule Port UDP 1434 Profile: Domain/Private	Used to locate other Ponemah workstations on the network.
SQL Server Browser Connect	Inbound Rule Port TCP 1433 Profile: Domain/Private	Used to locate other Ponemah workstations on the network.

Note: Windows 7 has the TCP 2869 port and UDP 1900 port opened only for the Profiles of Private and Domain, not for Public**.**

PONEMAH SERVICES

The following Services are installed during the installation of Ponemah. Their states will update upon Ponemah startup, depending on the acquisition interface currently selected.

Service Name	Default Setting	Comment
DSI Time Sync **(OpenART, MX2, CLC only)**	Automatic Started – Depends, see comments	Installed with Ponemah versions ≤5.20-SP8 and v5.30+ for synchronization between Ponemah hardwired and Implantable Telemetry (Data Exchange Matrix, MX2, CLC). **Started** for ACQ-7700 + OpenART, ACQ-16 + OpenART, ACQ-7700 + MX2, or ACQ-7700 + CLC SYNC systems **Stopped** if not a SYNC system.
DSI 7700 Time Sync **(OpenART, MX2, CLC only)**	Automatic Started – Depends, see comments	Installed with Ponemah versions 5.20 SP9 – SP11 for synchronization between Ponemah hardwired and MX2 or CLC. **Started** for ACQ-7700 + OpenART, ACQ-16 + OpenART, ACQ-7700 + MX2, or ACQ-7700 + CLC SYNC systems **Started** for ACQ-7700 + OpenART or ACQ-16 + OpenART, ACQ-7700 + MX2 or ACQ-7700 + CLC SYNC systems. **Stopped** if not a SYNC system.
DSIClock **(OpenART only)**	Automatic Started – Depends, see comments	Installed with OpenART. **Started** for OpenART. **Stopped** for SYNC systems, JET, CLC, and MX2 based systems. Windows Time needs to be Disabled for use with OpenART only.
Network Time Protocol Daemon **(CLC/MX2 only)**	Automatic Started – Depends, see comments	Installed with Ponemah. **Started** for CLC, MX2, and SYNC systems. **Stopped** for ACQ-7700, ACQ-16, JET, and OpenART systems.
SSDP Discovery	Automatic Started	Standard Windows Service. **Started** for CLC, MX2, APR, and JET systems. Does not impact ACQ-7700, ACQ-16 or OpenART.
UPnP Device Host	Automatic Started	Standard Windows Service. **Started** for CLC, MX2, APR, and JET systems. Does not impact ACQ-7700, ACQ-16 or OpenART.
P3Security	Automatic Started	Installed with Ponemah and used for Data Security.
Windows Time	Disabled Stopped	Installed with Windows. **Disabled** for OpenART, MX2, CLC, JET, Hardwired, and SYNC systems.

Service Name	Default Setting	Comment
SQL Server Browser	Automatic Started – Depends, see comments	Only needed if Ponemah's Study Protocol Option is being with multiple workstations (i.e. Network Study).

OTHER WINDOWS SETTINGS

The following settings are not automatically changed during installation or by Ponemah at startup but do have an impact on system performance. These settings must be changed before a reliable acquisition may be performed.

Feature	Update setting to:	Comment
Power: Put Computer to Sleep	Never	The computer should not be allowed go to sleep. Even in the High-Performance power plan it will be configured to sleep after 1 hour.
Power: Power Plan	High Performance	This helps with both Acquisition and Review performance. Windows 7 default is to power down after 15 minutes idle time. This will cause acquisition to stop.
Network Discover	Enable	When network discovery is ON, the computer can see other computers and network devices on the network. It is also visible to other network computers. For Ponemah v5.x, this is important to see other computers on the network when working with Network Study. It is also used to permit the system to locate MX2s, CLCs, APRs, and JET Receivers on the network for configuration. For Ponemah v6.x, this is important to permit the system to locate MX2s, CLCs, and APRs on the network for configuration.
Windows Search	Disable	Only allow searches or search indexing to occur when Ponemah is not running.
Windows Update	Disable	Only allow updates to be searched for, downloaded, and installed when Ponemah is not running.
Disk Defragmentation	Disable	Only allow defragmentation to occur when Ponemah is not running.
Windows Defender *(Windows 7)*	Disable	Only allow scanning to occur when Ponemah is not running.
Windows Defender Firewall *(Windows 10)*	Disable	Only allow scanning to occur when Ponemah is not running.
Windows Defender Antivirus Service *(Windows 10*	Disable	Only allow scanning to occur when Ponemah is not running.
Windows Defender Security Center Service	Disable	Only allow scanning to occur when Ponemah is not running.

Feature	Update setting to:	Comment
Automatic adjust clock for Daylight Saving Time	Depends on Ponemah version. See Comments.	If using Ponemah v5.x, this setting may be configured based on the researcher needs. ***However, if using the Study Protocol Option, the automatically adjust clock for Daylight Savings Time setting must be DISABLED***. If using Ponemah v6.x, the automatically adjust clock for Daylight Saving Time setting must be ***ENABLED***.

Please see Appendix for detailed instructions on how to configure these settings appropriately.

KNOWN 3RD PARTY PROBLEM EXECUTABLES

Any installed executable that uses system resources can impact the performance of the application. The following applications are known to cause issues that may impact performance and interrupt an acquisition.

Executable	Ideal State	Comment
Virus scanners	Disabled	If the virus scanner is required to be turned ON during acquisition, the Ponemah runtime folder and the Ponemah data folder must be excluded from scans. Virus Scanners are known to cause data buffer overflows due to their high system resource usage.
3rd Party Remote Desktop	Not used.	If the system is being accessed through a remote desktop application this can cause data buffer overflows due to the use of system resources.
Screensavers	Disabled	Screensavers should not be used. Screensavers that use OpenGL should be avoided.

PONEMAH EXECUTABLES

Below is a list of executables that may need to be added to an exception list for Ponemah to function correctly.

Executable	Comment
PPP3.EXE	Main Ponemah application which calls the other executables
JETRecTuner.exe	Needed for JET optimization call from Ponemah
CfgVideo.exe	Video configuration editor (non Noldus) called from Ponemah
DVR.exe	Video recorder (non Noldus) called from Ponemah
P3Player.exe	Video playback component called from Ponemah
Ponemah.ProcessUtilitesUI.exe	External application used for support
ArtDiag.exe	External application that runs OpenART diagnostics
CfgEdit.exe	Configuration application for OpenART called from Ponemah
CfgPrn.exe	Configuration print support for OpenART called from Ponemah
ProcessLogger.exe	Debugging utility used to determine cause of Data Buffer Overflows
Ponemah.SecurityApplication.exe	External application used to move Data Security settings between from one workstation to another

PONEMAH FOLDER PERMISSIONS

The following is a list of folders created during installation of Ponemah and the recommended permission settings for each. The LSS_P3_Administrator User and the P3_Users and P3_Administrator Groups are automatically created during installation.

If the system is being used in a GLP environment, the LSS_P3_Administrator User must be enabled and the Ponemah_Data folder permissions should be updated to the permission outlined below for Secured.

Folder	User Groups – Permissions	Comment
C:\Ponemah	P3_Users – Full control P3_Administrators – Full control	This is the main application runtime folder. The P3_Users and P3_Administrators User Groups are automatically added to this folder during the Ponemah installation process.
C:\Ponemah_Data	**Non-secured** P3_Users – Full Control P3_Administrators – Full control **Secured (GLP)** P3_Users – Read & execute, List folder contents, Read P3_Administrators – Full control	This is the folder which all Ponemah data is stored. For a non-secured system, the P3_Users and P3_Administrators User Groups are automatically added to this folder during the Ponemah installation process. For a secured system, the Ponemah Administrator may use the **Secure Existing Directory** function within the Ponemah Admin application to delete the current Users and add the P3_User and P3_Administrators groups to this folder with the permission listed.
C:\ProgramData\DSI	Everyone – Full Control	This folder is used by the PhysioTel Digital and MX2 configurations for saving the inventory of devices.

REQUIRED 3RD PARTY SUPPORT APPLICATIONS

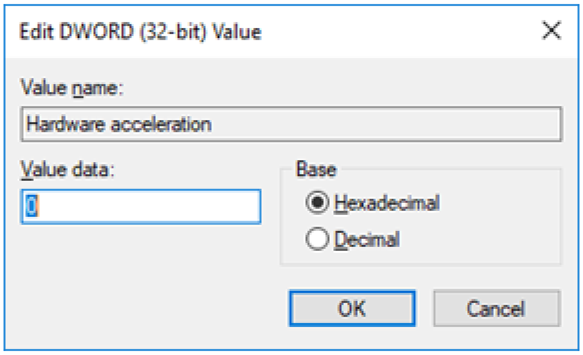
The following is a list of 3rd party applications needed by Ponemah to perform certain functions.

Application	Function
Internet Explorer (IE11) 11 or newer	IE11 is needed to run the Diagnostic web page for the PhysioTel Legacy/HD MX2 or PhysioTel Digital CLC devices. Without IE11, troubleshooting the telemetry interfaces and implants will not be possible. If an earlier version of IE is used, certain parts of the Diagnostics web page will not render correctly.
Microsoft Office 2013 or newer *(Optional)*	The Ponemah application generates Excel or Access based files and Office is only needed if there is a need to view those files on the Ponemah workstation.

NOLDUS MEDIA RECORDER REGISTRY UPDATE

If using Noldus Media Recorder, the following registry entry should be updated:

1. Open a command window by clicking on the start button and typing “regedit” in the search window
2. Select the **regedit** program.
3. Navigate to:
   [HKEY_CURRENT_USER\Software\MainConcept\MainConcept AVC/H.264 Video Decoder\MediaRecorder.exe]
4. Double-click **Hardware Acceleration.**
5. Change the *Value data* to **0**.



Value name: Hardware acceleration

Value data: 0

Base: ● Hexadecimal ○ Decimal

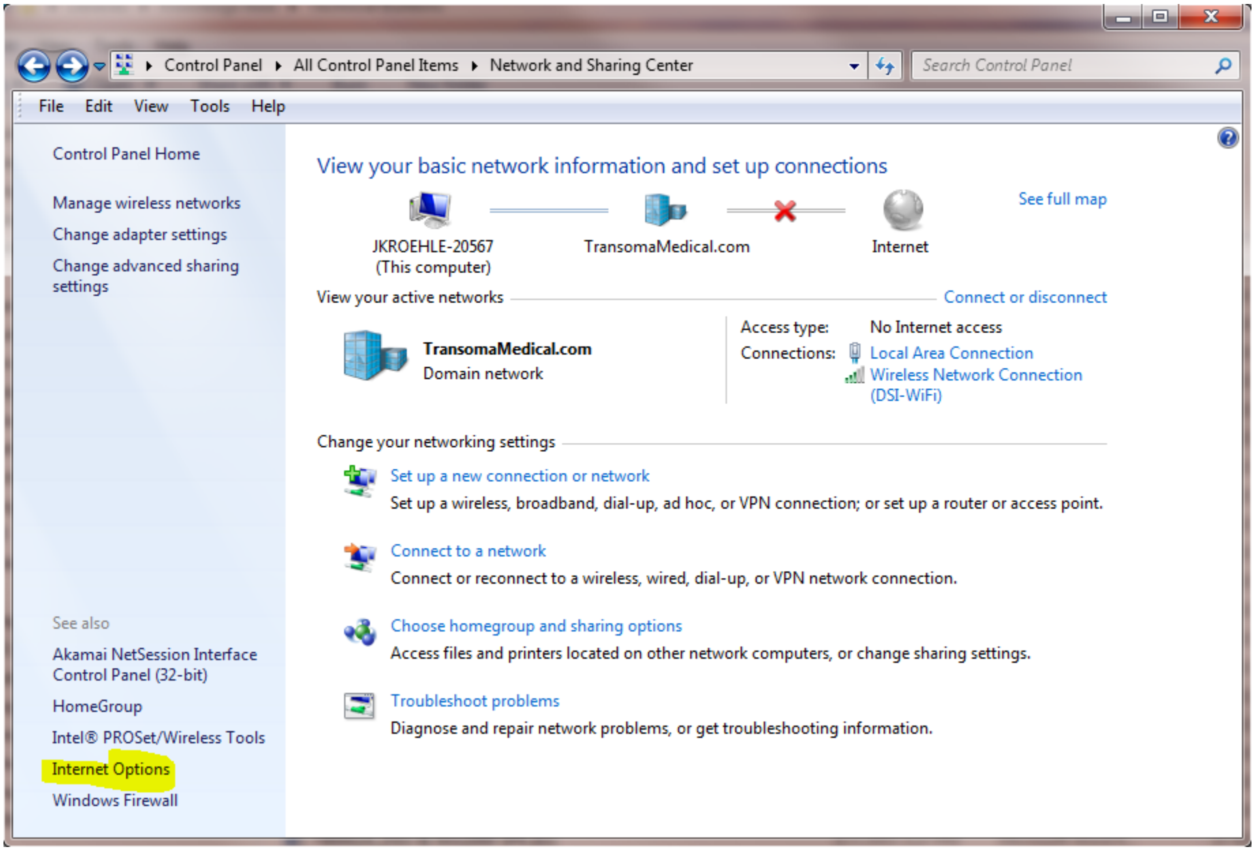
6. Click **OK**.
7. Close the Registry.

INTERNET EXPLORER PROXY SERVER

If the local network is setup to use a Proxy Server, communications to the DSI CLC or MX2 may be blocked.

To verify that a Proxy Server is disabled:

1. Select the Windows Start menu.
2. Select **Control Panel – Network and Sharing Center**.
3. Select **Internet Options**.


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
See also
Akamai NetSession Interface Control Panel (32-bit)
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
Windows Firewall
See full map
JKROEHLE-20567 (This computer)
TransomaMedical.com
Internet
Connect or disconnect

View your basic network information and set up connections

View your active networks

TransomaMedical.com
Domain network

Access type: No Internet access
Connections: Local Area Connection
Wireless Network Connection (DSI-WiFi)

Change your networking settings

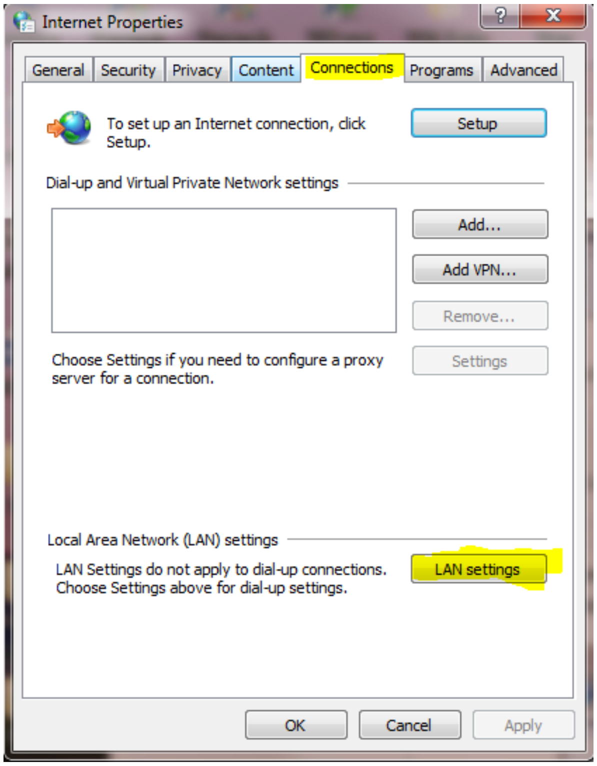
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

4. Select the **Connections** tab and then **LAN Settings**.



To set up an Internet connection, click Setup.

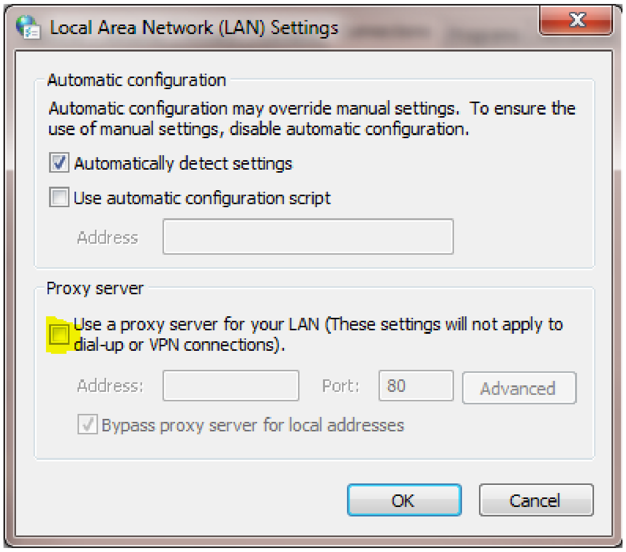
Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

5. Verify that the checkbox under the **Proxy server** section is not checked as displayed below. If it is checked, uncheck the setting and select **OK**.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

☑ Bypass proxy server for local addresses

6. Verify that communications to the MX2 or CLC has been restored.

DUAL NETWORK INTERFACE CARD (NIC) CONFIGURATION

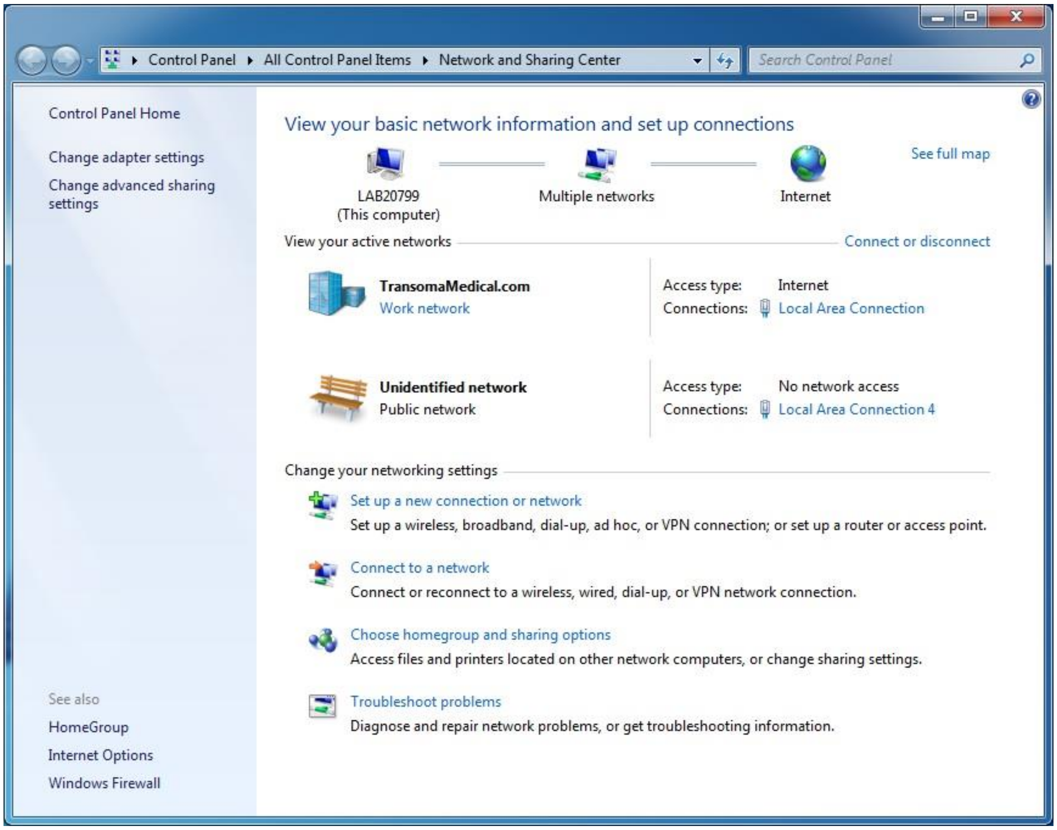
DSI recommends a second network interface card be used as part of the system configuration when using any acquisition interface that requires Ethernet communications (e.g. JET Bluetooth Receiver, CLC, or MX2).

One Ethernet card should be dedicated to the DSI telemetry system, which keeps the data acquisition samples isolated to the Ponemah workstation only. The second Ethernet card may be connected to the internal networking infrastructure for typical corporate/university use.

For the workstation to connect to the corporate/university network and have access to and communicate with the outside world, the network interfaces must be configured appropriately.

To appropriately configure the network interfaces:

1. Select the Windows **Start menu.**
2. Select **Control Panel | Network and Sharing Center**.
   Below is a typical dual network interface setup. The interface that needs to be verified for the correct configuration is **Local Area Connection 4**, which is the one connected to the DSI Telemetry equipment in this example. This may be different than what is displayed on other configured workstations.



View your basic network information and set up connections

View your active networks

TransomaMedical.com
Work network
Access type: Internet
Connections: Local Area Connection

Unidentified network
Public network
Access type: No network access
Connections: Local Area Connection 4

Change your networking settings

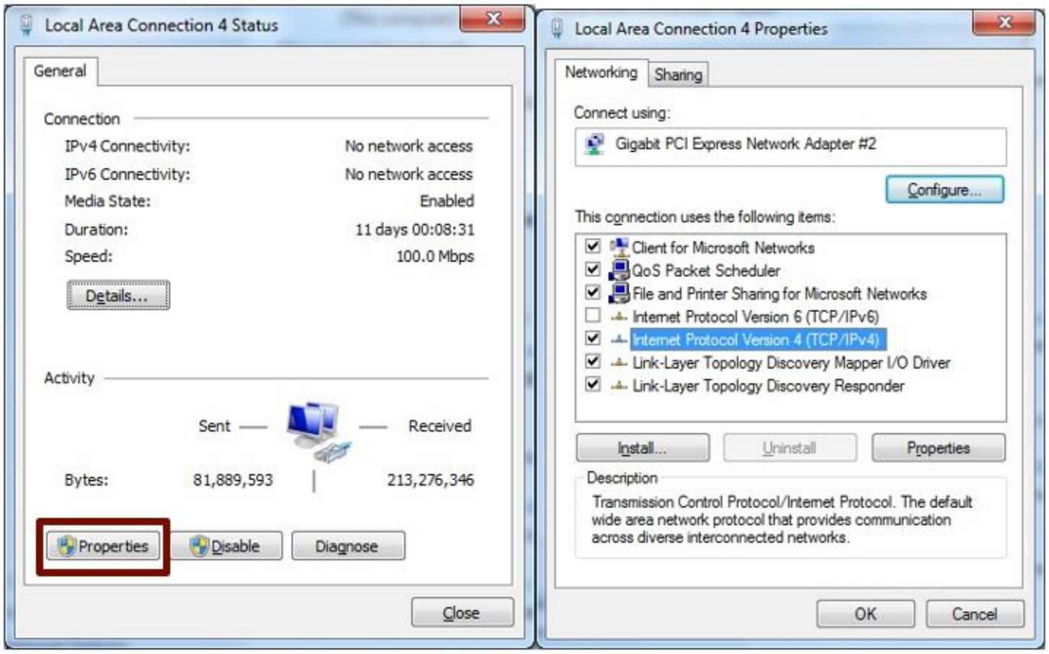
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Selecting that network will display the **Local Area Connection 4 Status** dialog as displayed below. Next, select **Properties**.



Local Area Connection 4 Status

General

Connection

IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	11 days 00:08:31
Speed:	100.0 Mbps

Details...

Activity

	Sent	Received
Bytes:	81,889,593	213,276,346

Local Area Connection 4 Properties

Networking Sharing

Connect using:

Gigabit PCI Express Network Adapter #2

Configure...

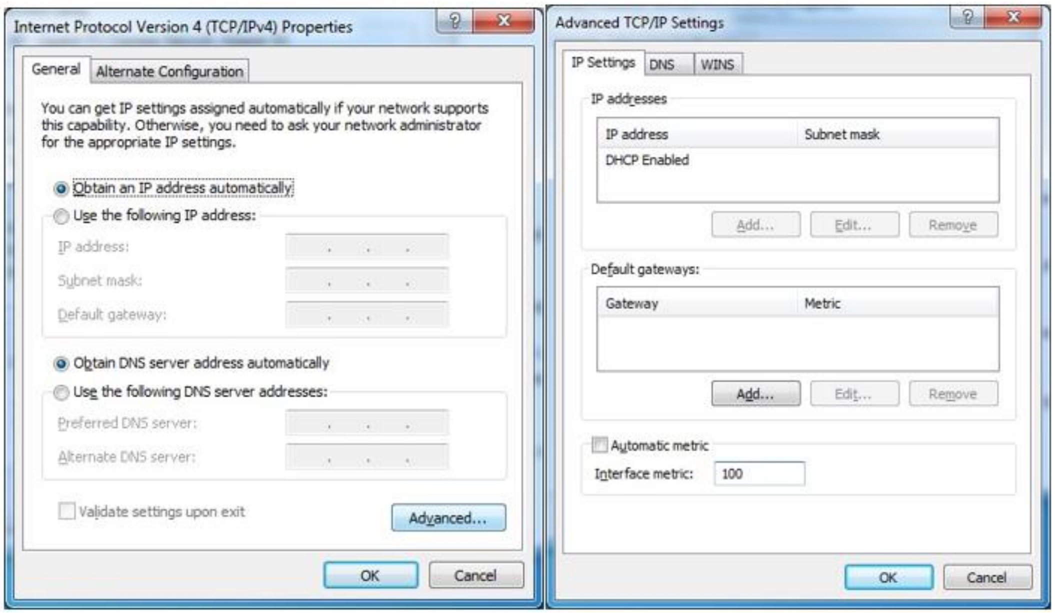
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. From the **Local Area Connection 4 Properties** dialog verify that **Internet Protocol Version 6 (TVP/IPv6)** is unchecked as displayed in the above dialog on the right.
5. Change the network metric such that it is higher than the metric for the network interface connected to the corporate/university network.
   a. Select **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**. Then, select **Advance…** to display the **Advance TCP/IP Settings**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address: . . .
  - Subnet mask: . . .
  - Default gateway: . . .
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced TCP/IP Settings

IP Settings DNS WINS

IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

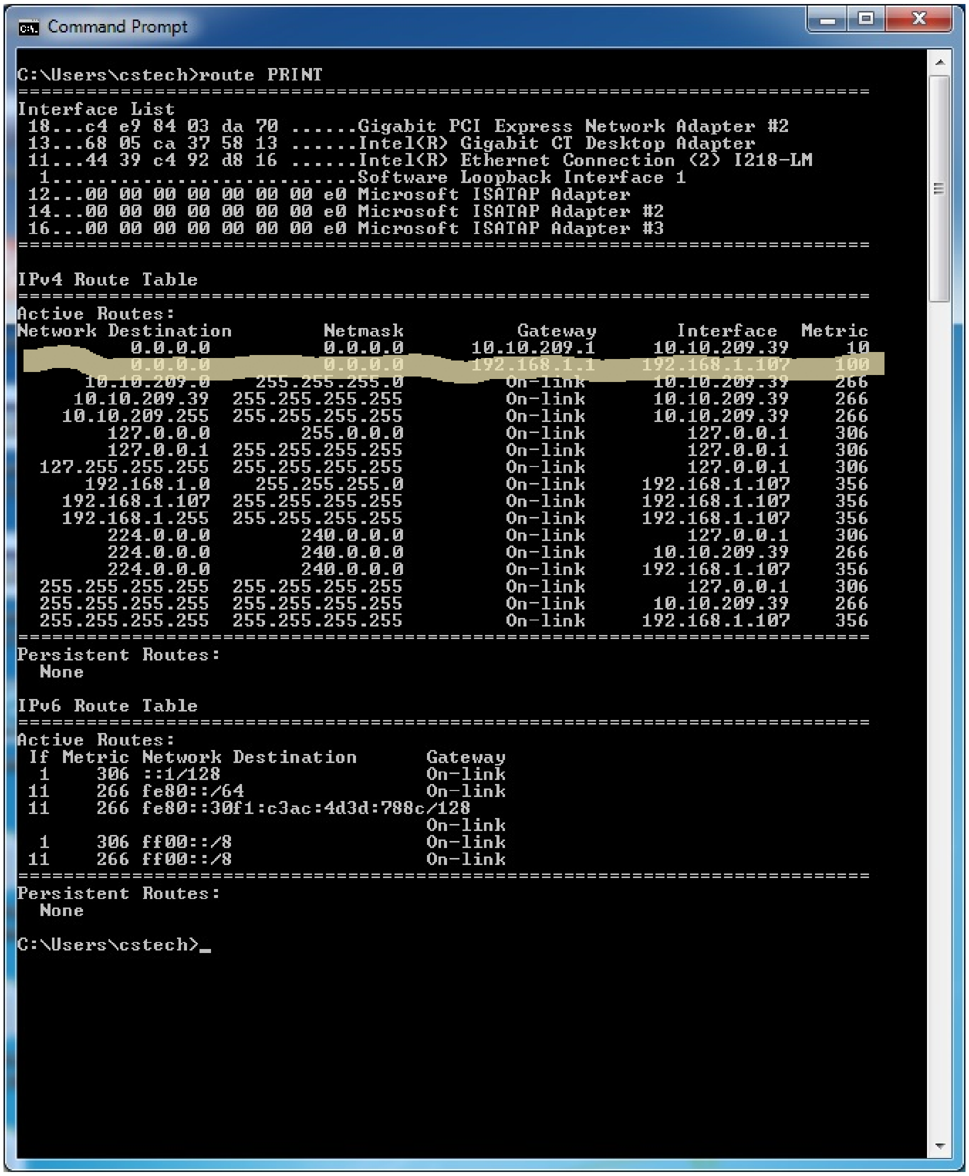
Gateway	Metric

☐ Automatic metric

Interface metric: 100

   b. Uncheck the **Automatic Metric** and enter **100** in the **Interface metric**, as displayed in the above dialog on the right.
   c. Click **OK** on each dialog until all the dialog windows are closed.

6. From a **Command Prompt**, type in **route PRINT** to display the network routing table on the workstation. For proper networking to the corporate/university network, the network interface must be a lower value than the DSI Telemetry network interface. In the example below the corporate network **Metric** is **10** which will allow the proper communication to occur within the corporate/university infrastructure.



```
C:\Users\cstech>route PRINT
===========================================================================
Interface List
 18...c4 e9 84 03 da 70 ......Gigabit PCI Express Network Adapter #2
 13...68 05 ca 37 58 13 ......Intel(R) Gigabit CT Desktop Adapter
 11...44 39 c4 92 d8 16 ......Intel(R) Ethernet Connection (2) I218-LM
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.10.209.1     10.10.209.39     10
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.107    100
      10.10.209.0    255.255.255.0         On-link      10.10.209.39    266
     10.10.209.39  255.255.255.255         On-link      10.10.209.39    266
    10.10.209.255  255.255.255.255         On-link      10.10.209.39    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link     192.168.1.107    356
    192.168.1.107  255.255.255.255         On-link     192.168.1.107    356
    192.168.1.255  255.255.255.255         On-link     192.168.1.107    356
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      10.10.209.39    266
        224.0.0.0        240.0.0.0         On-link     192.168.1.107    356
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      10.10.209.39    266
  255.255.255.255  255.255.255.255         On-link     192.168.1.107    356
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 11    266 fe80::/64                On-link
 11    266 fe80::30f1:c3ac:4d3d:788c/128
                                    On-link
  1    306 ff00::/8                 On-link
 11    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\cstech>_
```

Note: Using VPN can be problematic due to the tunneling by the VPN connection. If a VPN connection is required, make sure that the DSI Telemetry network interface has a greater metric then the VPN network.

OPTIONAL CONFIGURATION ITEMS

The following are optional recommendations used to more easily work with and troubleshoot the workstation.

INSTALL THE ACCESS DATABASE ENGINE

The AccessDatabaseEngine will allow researchers to use Excel 2007 or newer with Ponemah Excel output files if using Ponemah versions ≤v5.20.

1. Locate the **AccessDatabaseEngine.exe** Program. It can either be found on the Ponemah install disk, on the Ponemah Service Pack disk. It may also be downloaded from the following link.
   a. https://datasci.box.com/v/AccessDatabaseEngine
2. Double-click the file name.
3. If the window from **User Account Control** (which may or may not be minimized) asks for permission to install, select **Yes**.
4. Select **Next.**
5. Check **I accept the terms in the License Agreement**, select **Next,** and then select **Install**.
6. When installation finishes select **OK**.
7. Close window.

CONFIGURING USERS FOR PONEMAH DATA SECURITY OPTION (DSO)

The Ponemah Data Security Option (DSO) is used to assist an FDA- regulated organization achieve compliance with 21 CFR Part 11 regulations. The Data Security Option utilizes local Windows® User accounts, passwords, and Microsoft's Windows NTFS file system to provide control over the integrity of electronic records generated by the Ponemah application, allow Users to electronically sign records, and limit system access and operation(s) to only authorized individuals.

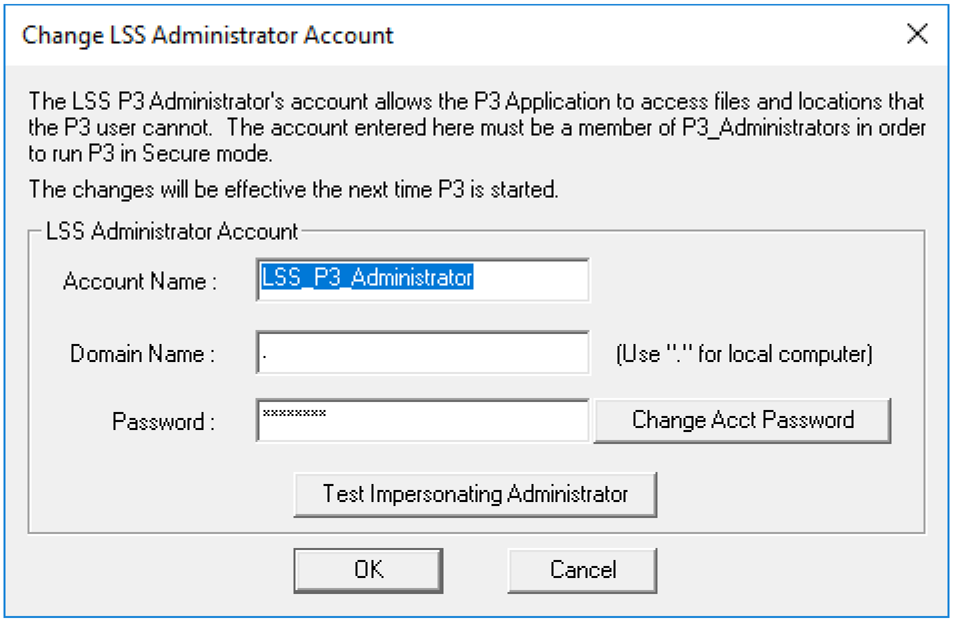
UNDERSTANDING PONEMAH USERS AND GROUPS

During the Ponemah installation process, Ponemah creates the following accounts:

Account Name	Account Type	Purpose
LSS_P3_Administrator*	Local User	Member of the Administrator and P3_Administrators Groups. Used by the Ponemah application to impersonate a local administrator to access and create files and locations P3_Users cannot. *Note: This account is disabled by default and must be enabled by a Windows Administrator to use the DSO.*
P3_Administrators	Local Group	When using DSO, Users (Domain or Local) added to this Group will be permitted access to run the Ponemah Admin Program. Users must also be a part of the P3_Users Group. It is recommended that only non-Ponemah Users (such as IT personnel) have access to the Ponemah Admin application to control the following responsibilities: • Secure the system and setup security controls. • Grant Ponemah Users (those involved in running the Ponemah application to execute studies) authority to use the system.

P3_Users	Local Group	Users or Groups (Domain or Local) involved in running the Ponemah application to execute studies should be added to this Group by the Ponemah Administrator. Once added, these Users will be listed in the Ponemah Admin application's User List. The Ponemah Administrator may then grant these Users access to the Ponemah application and assign access levels permissions to Ponemah operations. Those added to the P3_Users Group generally do not have Administrator privileges to the workstation, but instead have normal User privileges. This is to ensure the integrity of the application and the data that is collected and analyzed by Ponemah.

*In many cases, the LSS_P3_Administrator must be a Domain admin to access files and locations across company/university networks. The LSS_P3_Adminstrator account may be changed using the Ponemah Admin application to appropriately configure the Account Name, Domain, and/or Password with appropriate write access to the network folder. Once the account information is updated, click the **Test Impersonating Administrator** button to verify Ponemah can login to the account. Please see the DSO User Manual (MU00169) for more details.



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 : ********* Change Acct Password

Test Impersonating Administrator

OK Cancel

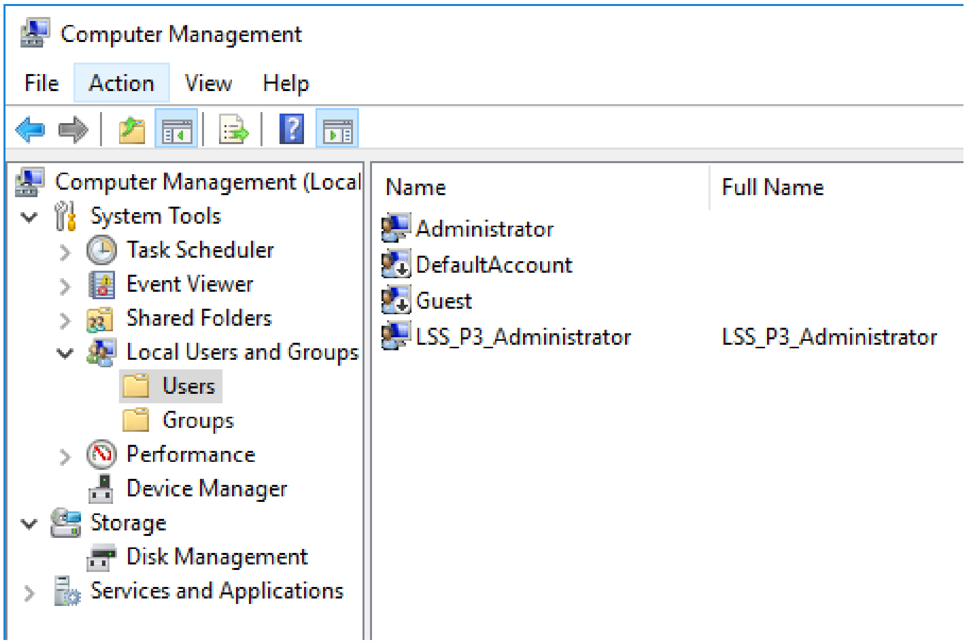
ENABLING THE LSS_P3_ADMINISTRATOR ACCOUNT

Note: Only Windows Users with Administrator privileges may enable Local User Accounts.

To enable the LSS_P3_Administrator:

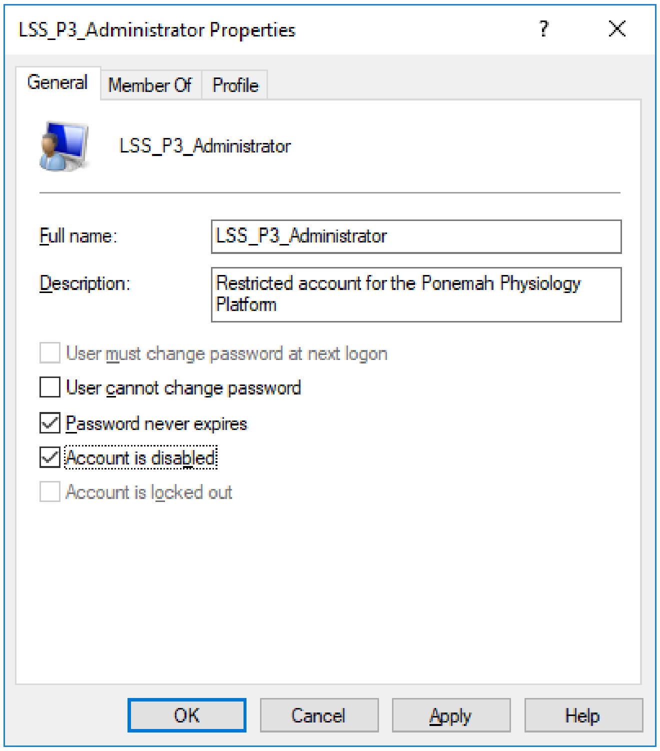
1. Navigate to the Computer Management.
    a. Windows 7
        i. Select the **Windows Orb** (the **Start** button).
        ii. Right-click **Computer** and select **Manage**.
    b. Windows 10
        i. Enter **Computer Management** into the **Search Bar**.
        ii. Select **Computer Management**.

2. Expand **Local Users and Groups** from the tree view on the left side of the *Computer Management* dialog.



Name	Full Name
Administrator	
DefaultAccount	
Guest	
LSS_P3_Administrator	LSS_P3_Administrator

3. Double-click **LSS_P3_Administrator**.



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

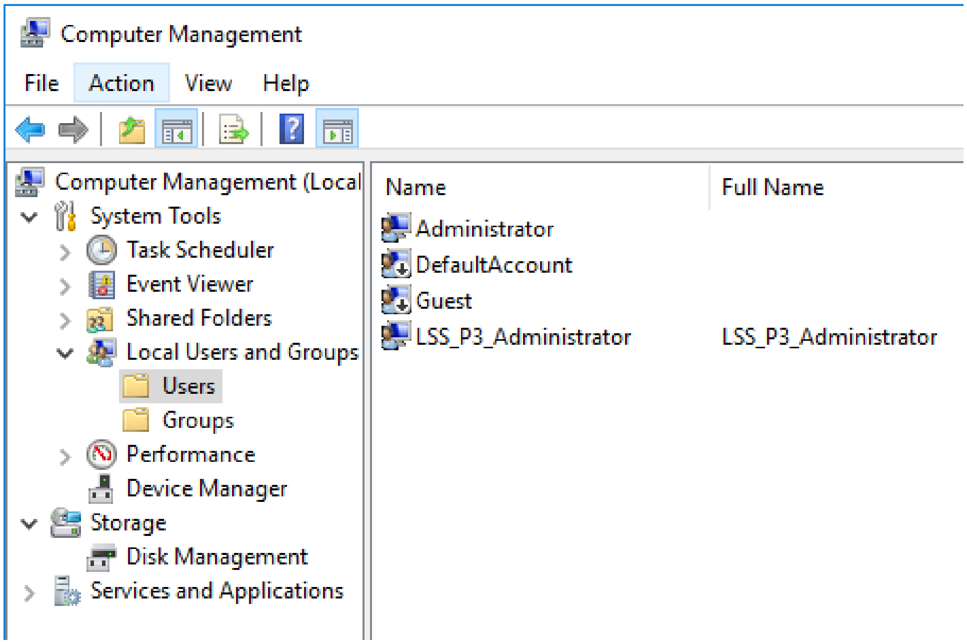
4. **Uncheck** the **Account is disabled** checkbox.
5. Click **OK**.

ADDING USERS AND GROUPS TO THE P3_USERS GROUP

Note: Only Windows Users with Administrator privileges may add Users to the P3_User Group.

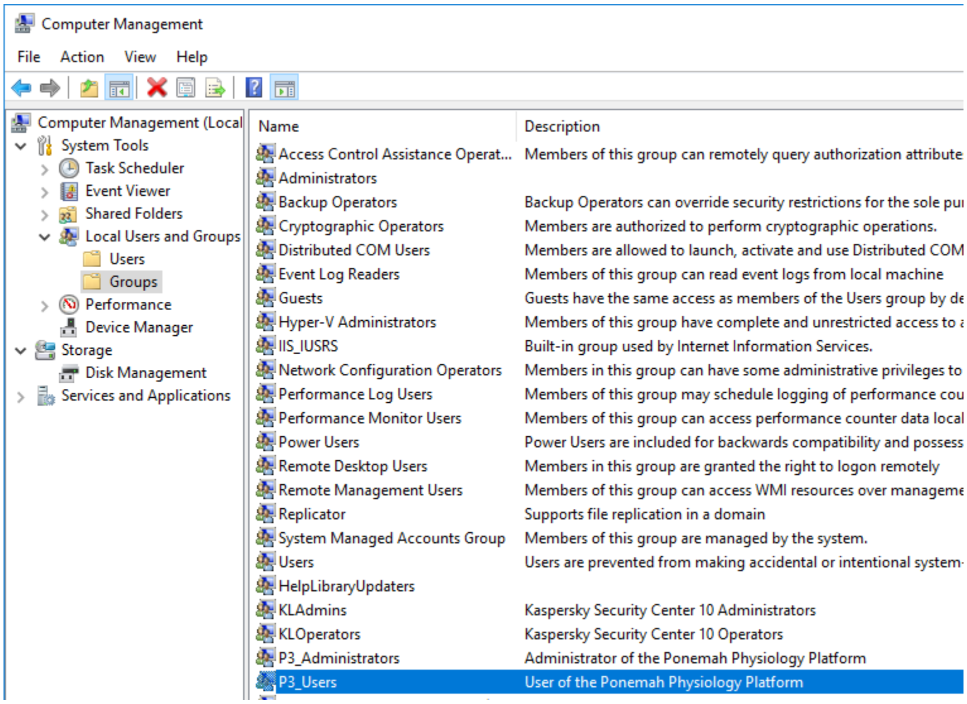
To add users:

6. Navigate to the Computer Management.
    a. Windows 7
        i. Select the **Windows Orb** (the **Start** button).
        ii. Right-click **Computer** and select **Manage**.
    b. Windows 10
        i. Enter **Computer Management** into the **Search Bar**.
        ii. Select **Computer Management**.
7. Expand **Local Users and Groups** from the tree view on the left side of the *Computer Management* dialog.



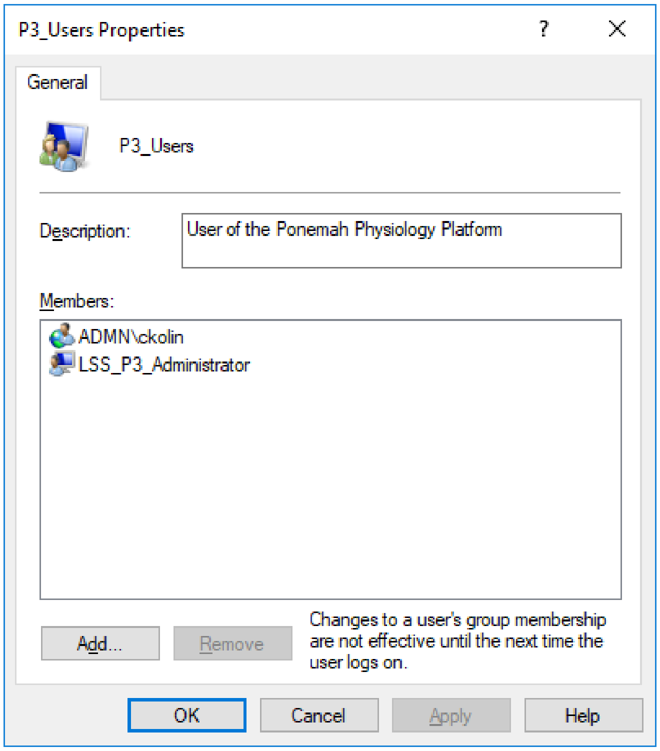
Name	Full Name
Administrator	
DefaultAccount	
Guest	
LSS_P3_Administrator	LSS_P3_Administrator

8. Select the **Groups** folder.



Name	Description
Access Control Assistance Operat...	Members of this group can remotely query authorization attribute
Administrators	
Backup Operators	Backup Operators can override security restrictions for the sole pu
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by de
Hyper-V Administrators	Members of this group have complete and unrestricted access to a
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to
Performance Log Users	Members of this group may schedule logging of performance cou
Performance Monitor Users	Members of this group can access performance counter data local
Power Users	Power Users are included for backwards compatibility and possess
Remote Desktop Users	Members in this group are granted the right to logon remotely
Remote Management Users	Members of this group can access WMI resources over manageme
Replicator	Supports file replication in a domain
System Managed Accounts Group	Members of this group are managed by the system.
Users	Users are prevented from making accidental or intentional system-
HelpLibraryUpdaters	
KLAdmins	Kaspersky Security Center 10 Administrators
KLOperators	Kaspersky Security Center 10 Operators
P3_Administrators	Administrator of the Ponemah Physiology Platform
P3_Users	User of the Ponemah Physiology Platform

9. Double-click the **P3_Users** group.



P3_Users

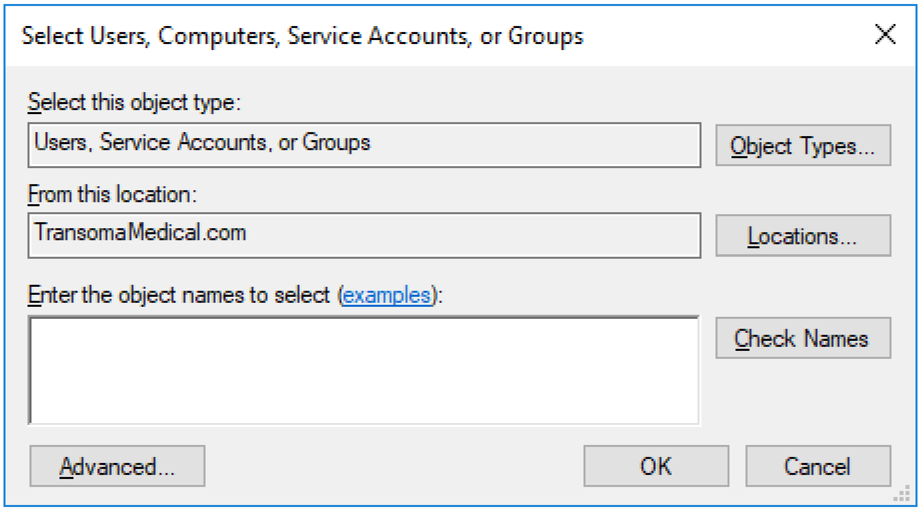
Description: User of the Ponemah Physiology Platform

Members:

ADMN\ckolin
LSS_P3_Administrator

Changes to a user's group membership are not effective until the next time the user logs on.

10. Click the **Add** button to add Domain or Local Users or Groups.



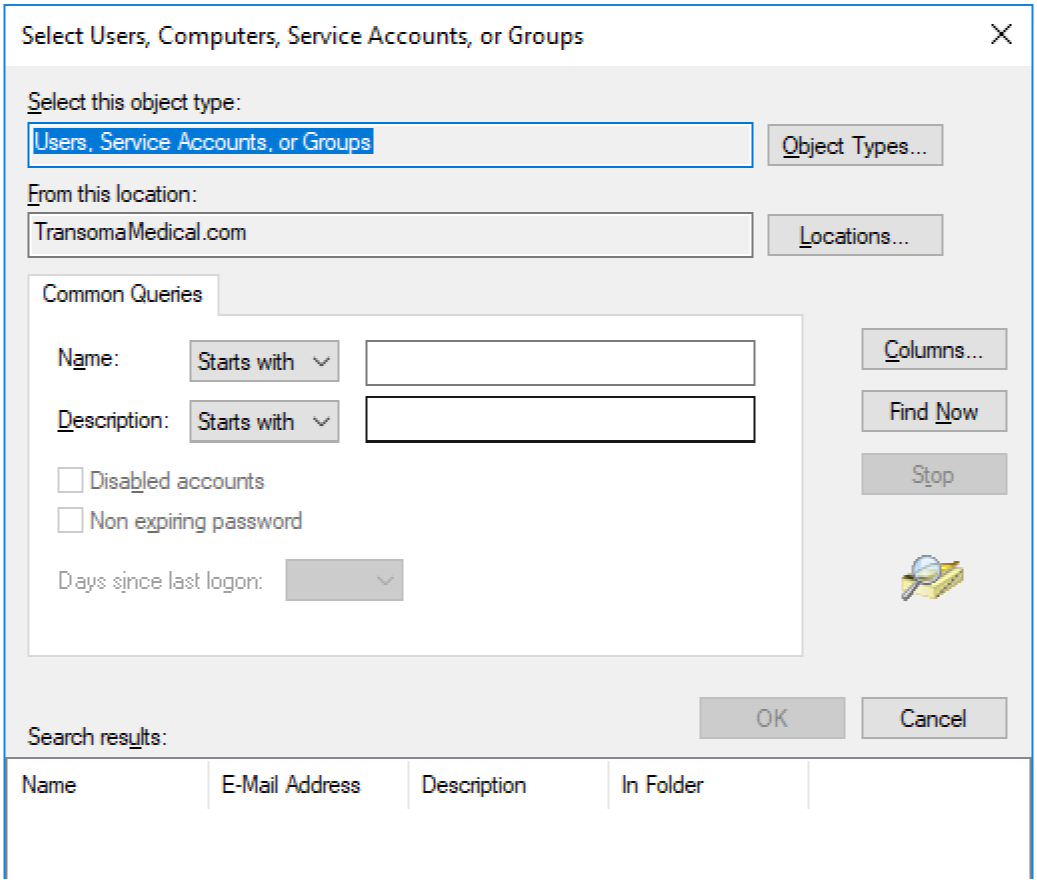
Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, or Groups

From this location: TransomaMedical.com

Enter the object names to select (examples):

11. Click Advanced to more easily search User and Groups.



Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, or Groups

From this location: TransomaMedical.com

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

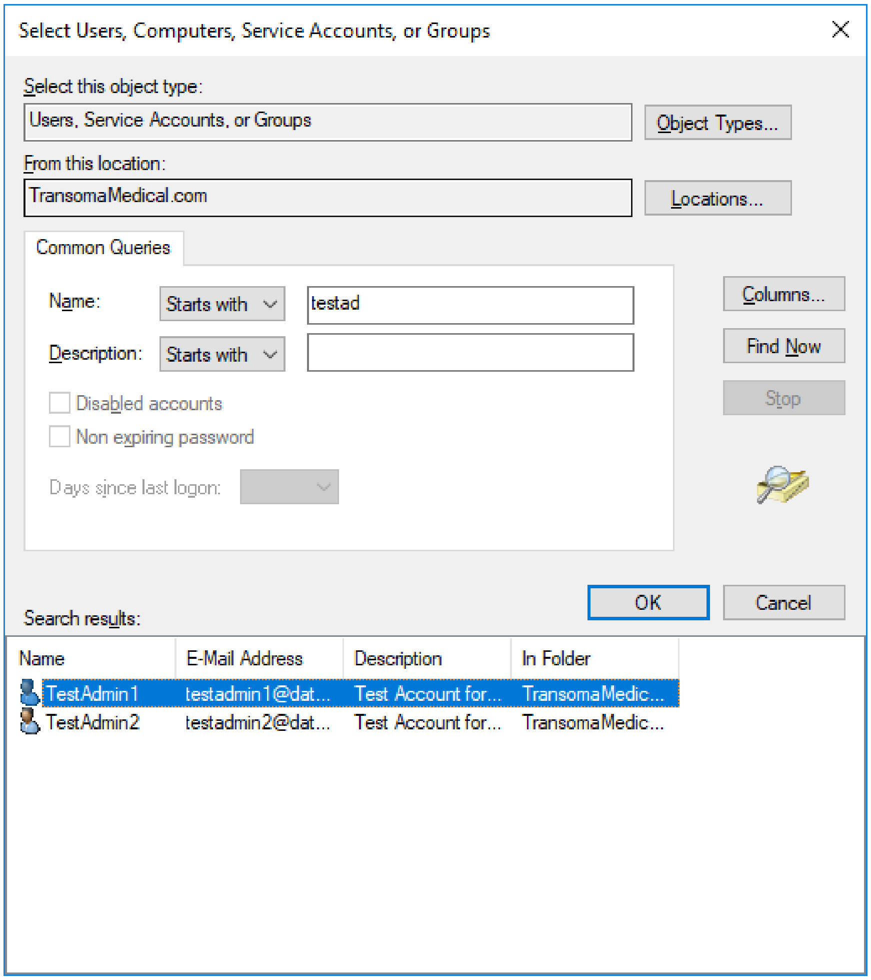
Days since last logon:

Search results:

Name	E-Mail Address	Description	In Folder

12. Click the **Locations** button and select the Domain If the workstation is part of a Domain and the User(s) or Group(s) reside in an Active Directory Domain account. If the workstation is a local system, then select the computer name in **Locations** to add a local User.

13. Enter a portion of the User or Group name to be added to the P3_Users group, then click **Find Now**. In the image below **testad** was searched for and from the **Search results** the User or Group name(s) can be selected.



Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, or Groups

From this location: TransomaMedical.com

Common Queries

Name: Starts with — testad

Description: Starts with

□ Disabled accounts

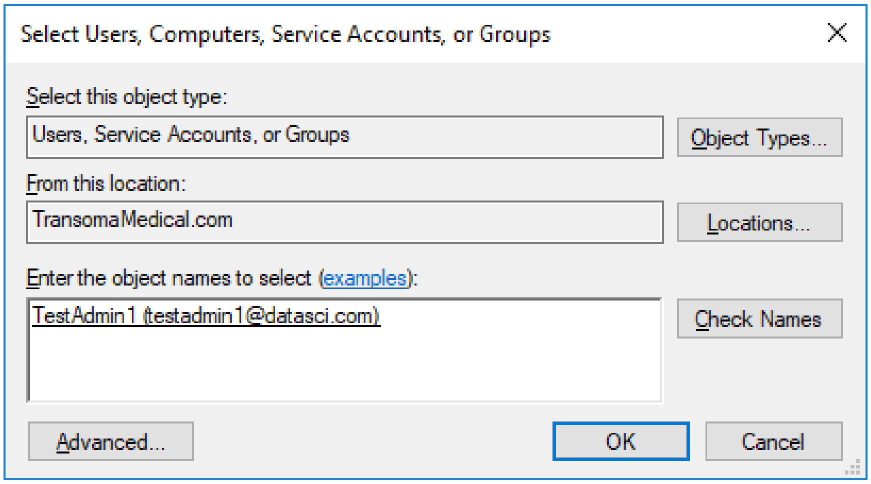
□ Non expiring password

Days since last logon:

Search results:

Name	E-Mail Address	Description	In Folder
TestAdmin1	testadmin1@dat...	Test Account for...	TransomaMedic...
TestAdmin2	testadmin2@dat...	Test Account for...	TransomaMedic...

14. Click **OK** to add to the P3_Users group.



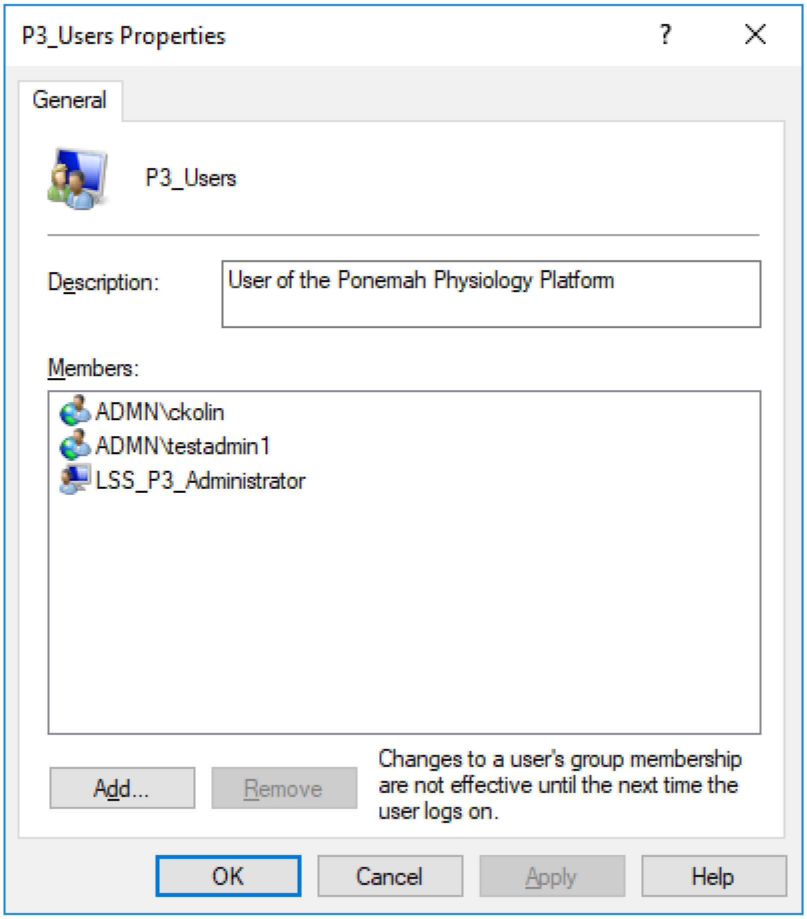
Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, or Groups

From this location: TransomaMedical.com

Enter the object names to select (examples): TestAdmin1 (testadmin1@datasci.com)

15. Click **OK**.



Description: User of the Ponemah Physiology Platform

Members:

ADMN\ckolin

ADMN\testadmin1

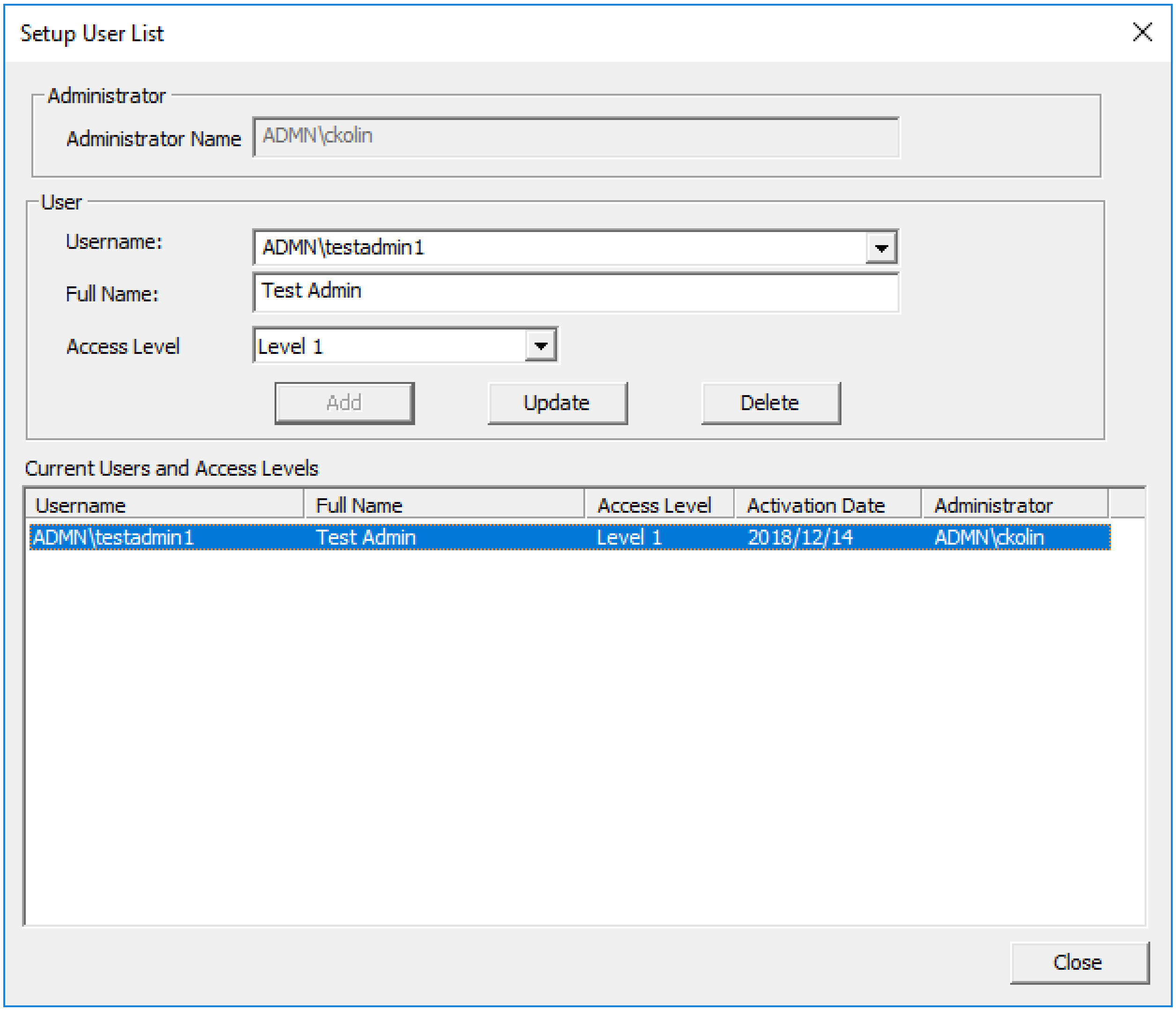
LSS_P3_Administrator

Changes to a user's group membership are not effective until the next time the user logs on.

16. Click **OK**.

The Ponemah Administrator can now add the User to the Data Security User List using the Ponemah Admin application. Please see the DSO User Manual (MU00169) for details on using the Ponemah Admin program to configure Access Levels and Secure Directories. Please see the

Ponemah Folder Permissions section of this manual for additional details.



User

Administrator Name: ADMN\ckolin

Username: ADMN\testadmin1

Full Name: Test Admin

Access Level: Level 1

Current Users and Access Levels

Username	Full Name	Access Level	Activation Date	Administrator
ADMN\testadmin1	Test Admin	Level 1	2018/12/14	ADMN\ckolin

CONFIGURING THE PHYSIOTEL SYSTEM TO STATIC IP ADDRESSES

By default, PhysioTel, PhysioTel HD, and PhysioTel Digital (PTD) network devices are configured to use Dynamic IP addresses. This requires a DHPC server to be in place to assign IP addresses to these network devices. The simplest means to add a DHCP server to a dedicated network is to use a router, which has this feature built in.

Some users may wish to use Static IP address instead of Dynamic for reduced system complexity. To do this, the following network devices need to be reconfigured to use a Static IP in the order listed:

1. Matrix 2.0 (MX2)/Communication Link Controller (CLC)
2. E2S-1/APR-1
3. Acquisition Computer

The IP addresses configured can include the following selections as these are private addresses:

- 10.0.0.0 to 10.255.255.255

- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Consult with your IT group for any questions regarding which IP addresses to use. View the web site ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt for information on private addresses.

The following sections will provide step-by-step instruction on how to reconfigure the PTD system network devices for a Static IP network configuration.

For the purposes of this technical note, the network devices will be configured to the network settings listed below. The PTD CLC will be used in this example, however the same process will work with the PhysioTel and PhysioTel HD MX2.

- IP Address
  - CLC: 10.1.1.1
  - E2S-1: 10.1.1.10
  - Acquisition Computer: 10.1.1.11
- Subnet mask:
  - 255.255.255.0
- Gateway:
  - *[leave blank]*

Note: Reconfiguration will need to occur from a network containing a DHCP server in order to initially locate the network devices.

MX2/CLC STATIC IP ADDRESS CONFIGURATION

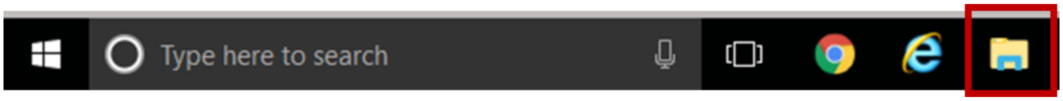
This section provides instructions on how to configure an MX2 or a CLC to use a Static IP address.

Note: The CLC will be used as the example in the steps below; however, the same steps apply to the MX2.

1. Connect the CLC(s) to the network.
2. Windows 7 - Click on the **Windows Orb** (the **Start** button) and select **Computer**.

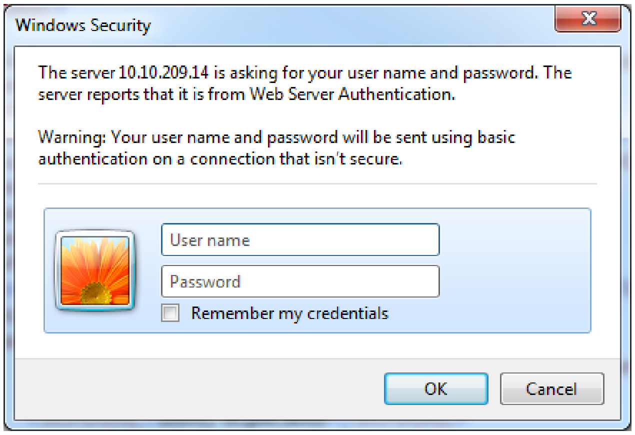
   OR

   Windows10 – Click the File Explorer.

3. From the menu pane on the left of the dialog, scroll down and select **Network** from the list.
4. From the pane on the right, under the *Other Devices* heading, the CLCs connected to the network will be seen.
5. **Right-click** on the CLC you would like to reconfigure and select Properties.
6. **Locate the** IP address within the dialog.
7. Launch Mozilla Firefox or Internet Explorer 11.

8. Enter http://x.x.x.x/ into the address bar, where x.x.x.x is the IP address obtained from the CLC Properties dialog.
9. Strike the <Enter> key to launch the Web Security dialog for authentication.

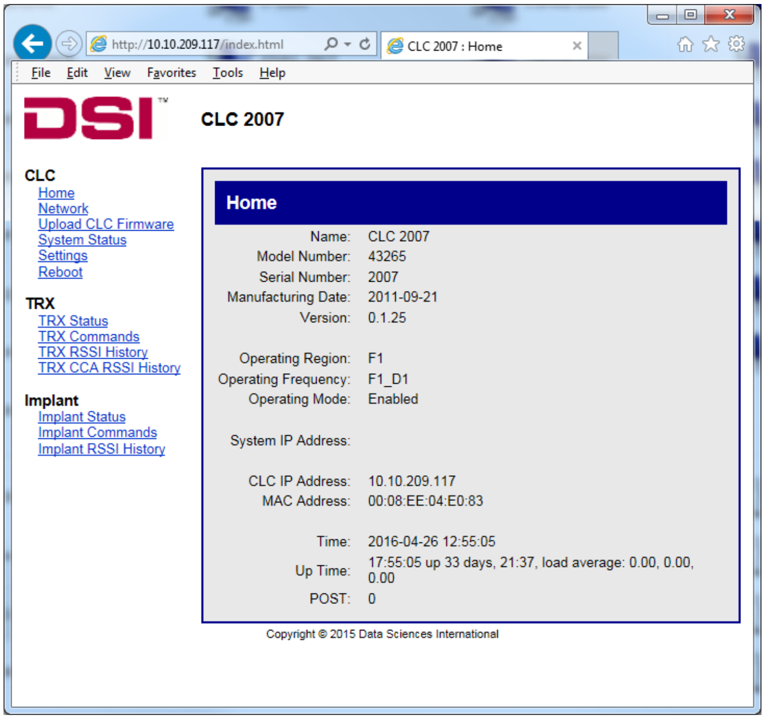


Windows Security

The server 10.10.209.14 is asking for your user name and password. The server reports that it is from Web Server Authentication.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

10. Enter in the Diagnostic username and password for the CLC.
    a. Username: *Diag* (username is case sensitive)
    b. Password: *[leave blank]*
11. The **Home** page of the *CLC Diagnostics* webpage should be displayed.



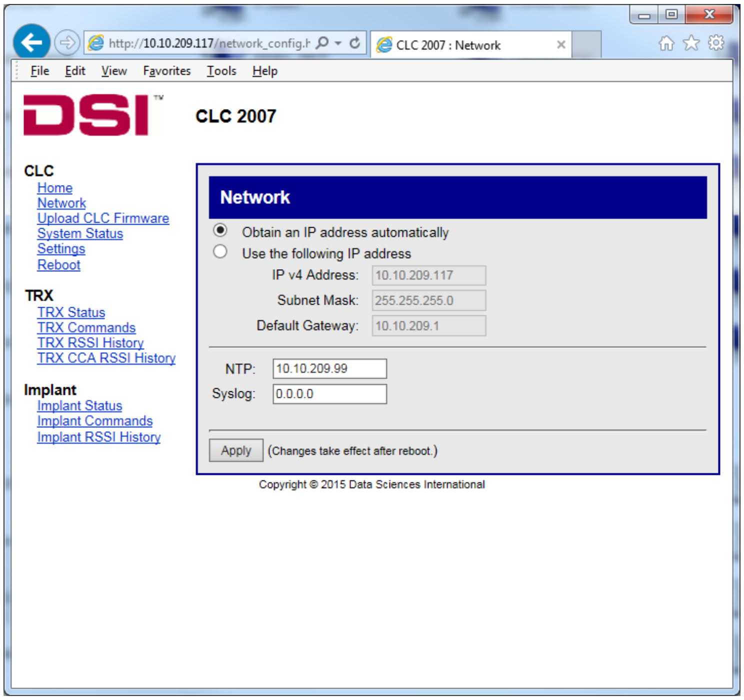
CLC 2007

Home

Name:	CLC 2007
Model Number:	43265
Serial Number:	2007
Manufacturing Date:	2011-09-21
Version:	0.1.25
Operating Region:	F1
Operating Frequency:	F1_D1
Operating Mode:	Enabled
System IP Address:	
CLC IP Address:	10.10.209.117
MAC Address:	00:08:EE:04:E0:83
Time:	2016-04-26 12:55:05
Up Time:	17:55:05 up 33 days, 21:37, load average: 0.00, 0.00, 0.00
POST:	0

Copyright © 2015 Data Sciences International

12. Select the **Network** link from the list on the left under the *CLC* header.



CLC 2007

Network

● Obtain an IP address automatically

○ Use the following IP address

IP v4 Address: 10.10.209.117

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.209.1

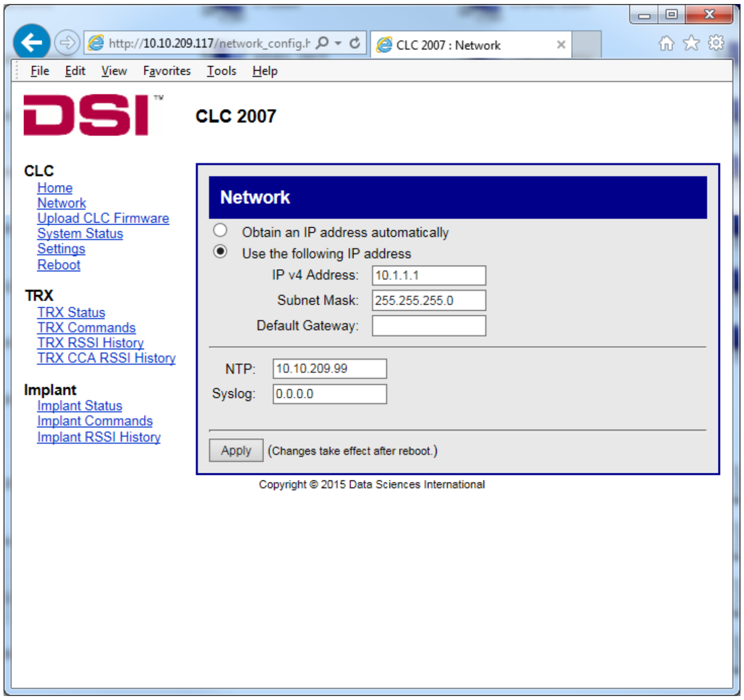
NTP: 10.10.209.99

Syslog: 0.0.0.0

Apply (Changes take effect after reboot.)

Copyright © 2015 Data Sciences International

13. Select the radio button associated with *Use the following IP address.*
14. Enter the desired **IP address**, **Subnet mask**, and **Default Gateway**.



CLC 2007

Network

○ Obtain an IP address automatically

● Use the following IP address

IP v4 Address: 10.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway:

NTP: 10.10.209.99

Syslog: 0.0.0.0

Apply (Changes take effect after reboot.)

Copyright © 2015 Data Sciences International

15. Click **Apply**.
16. Write down the serial number of the CLC and the Static IP address used for your records.
17. Repeat steps 4-14 for remaining CLCs.

Note: Be sure to use the same Subnet when configuring the IP address for any additional network device intended to be used with this system. In this example, we used the following IP address: 10.1.1.1. For additional CLCs, set the

IP address to the value 10.1.1.x where 'x' is any number between 2 and 254. The value of '1' cannot be used because the first CLC was configured to that address.

If the Static IP address is forgotten, the CLC may be reset back to a Dynamic IP configuration by holding the reset button for 5 to 15 seconds.

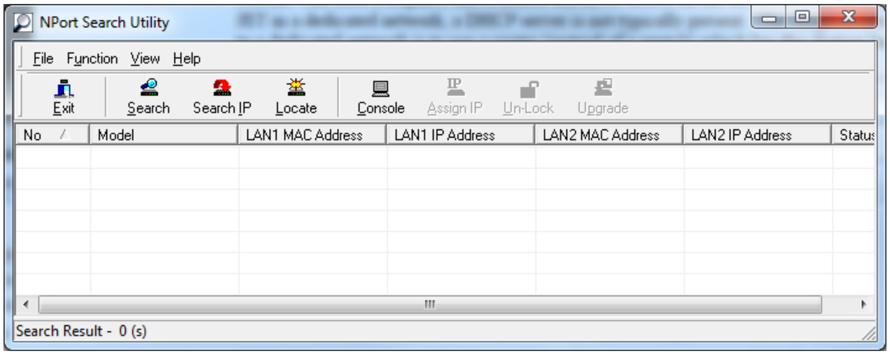
APR-2 STATIC IP ADDRESS CONFIGURATION

This section only needs to be completed if using implants containing a pressure sensor. If using an APR-1 for Ambient Pressure Reference, the E2S-1 is used to connect it to the network.

1. Connect the APR-2 (or E2S-1) to the network and apply power using either the dedicated power supply or a Power over Ethernet (PoE) switch.
2. Launch the **Nport Search Utility** application – *nplock.exe* – from the following location:
   a. Ponemah v6.x
      C:\Ponemah\Utils\NPort Search\
   b. Ponemah v5.3x
      C:\Ponemah\Utilities\E2SLocator\
   c. Internet Download
      http://www.moxa.com/support/sarch_result.aspx?prod_id=64&type_id=5&type=soft

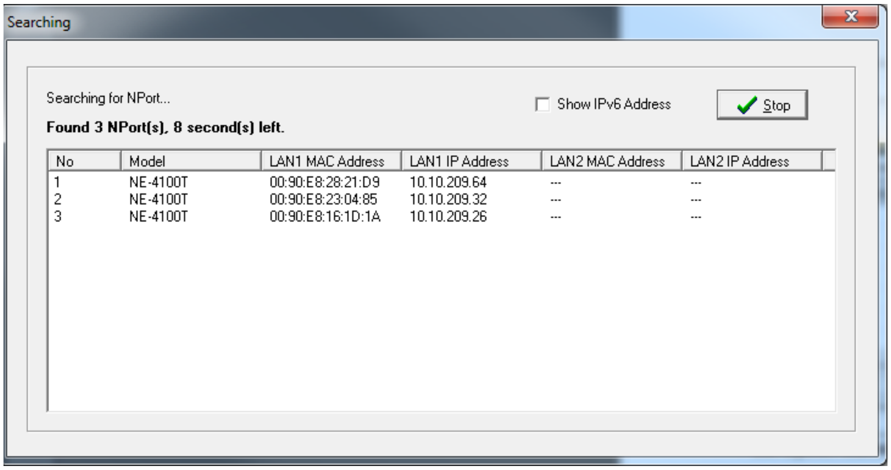
   The initial launch will prompt the user to install the program. Follow the on-screen instruction to complete this process.

3. One the Nport Search Utility is displayed, select the Search icon.



Search Result - 0 (s)

4. A status window will appear displaying that it is searching for NPorts.

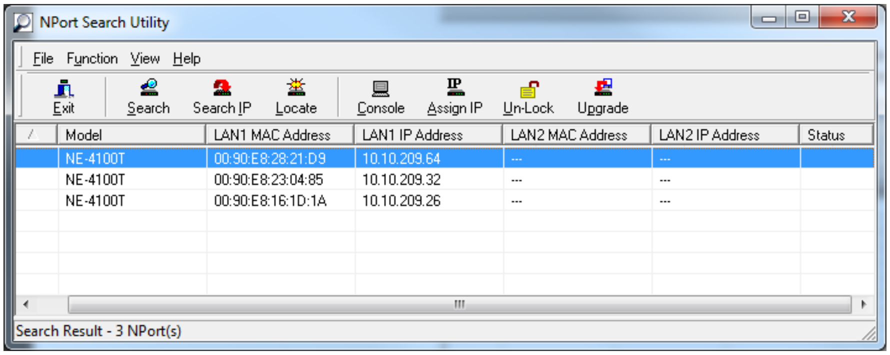


Searching for NPort...

Found 3 NPort(s), 8 second(s) left.

No	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address
1	NE-4100T	00:90:E8:28:21:D9	10.10.209.64	---	---
2	NE-4100T	00:90:E8:23:04:85	10.10.209.32	---	---
3	NE-4100T	00:90:E8:16:1D:1A	10.10.209.26	---	---

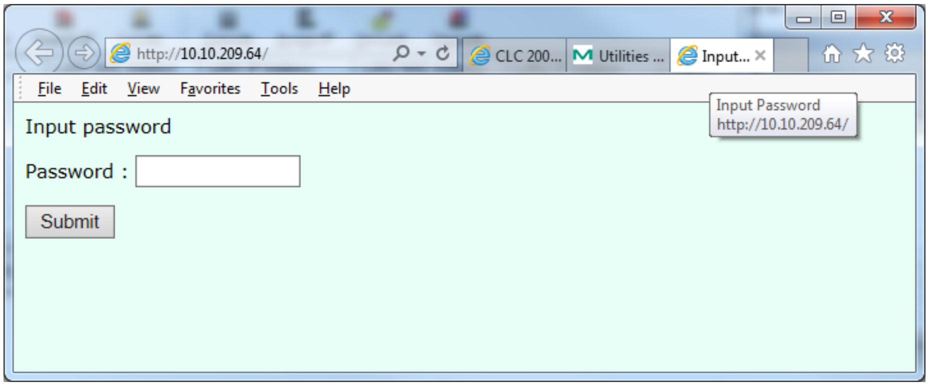
5. The NPort application window will then show all available Moxa NPorts. Double-click on the MAC Address that matches the APR-2 (or E2S-1) you need to modify.



/	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status
	NE-4100T	00:90:E8:28:21:D9	10.10.209.64	---	---	
	NE-4100T	00:90:E8:23:04:85	10.10.209.32	---	---	
	NE-4100T	00:90:E8:16:1D:1A	10.10.209.26	---	---	

Search Result - 3 NPort(s)

6. A webpage will be displayed requesting a password.



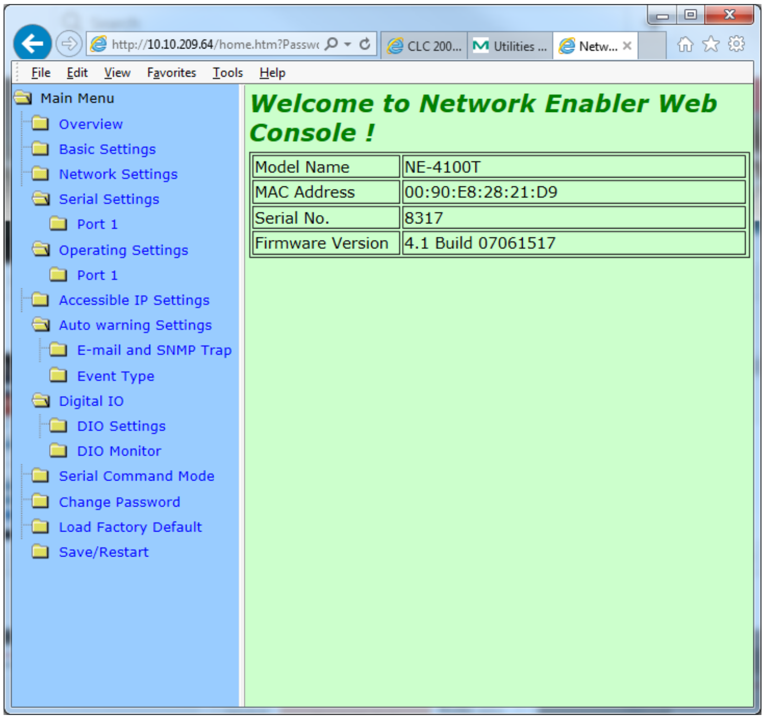
Input password

Password :

Submit

7. Enter the following password: *buffy*

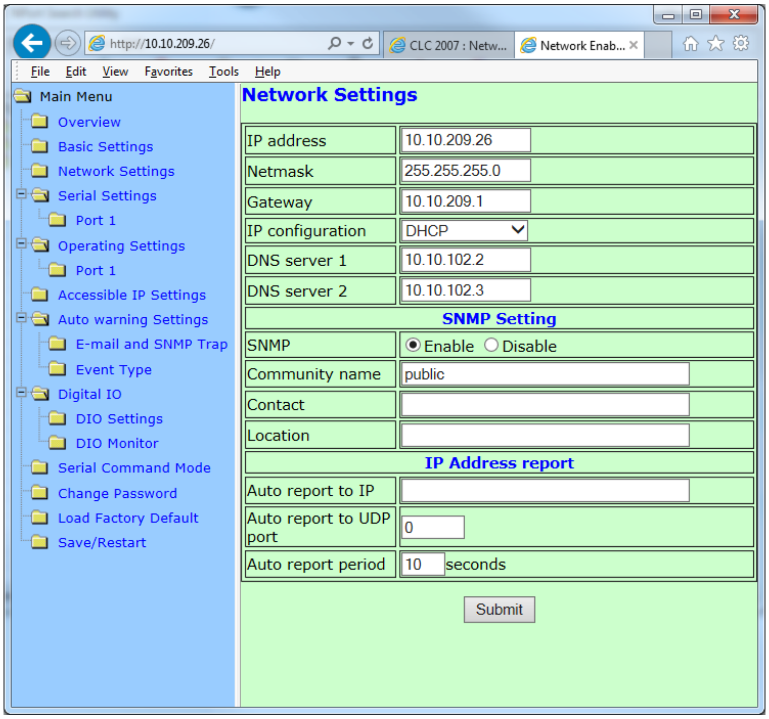
8. Select **Submit**



Welcome to Network Enabler Web Console !

Model Name	NE-4100T
MAC Address	00:90:E8:28:21:D9
Serial No.	8317
Firmware Version	4.1 Build 07061517

9. Select the **Network Settings** link from the tree view on the left side of the webpage.



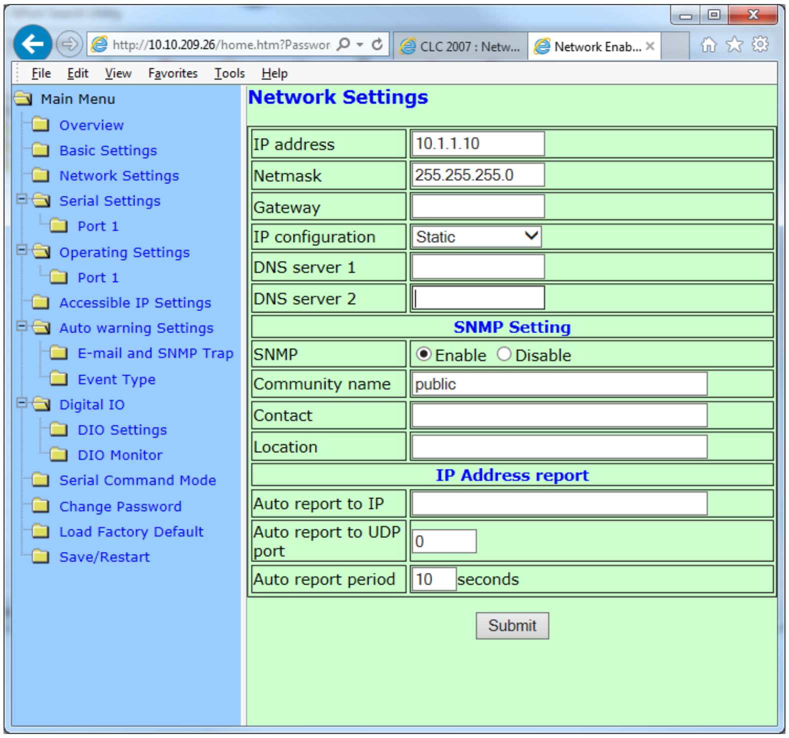
Network Settings

IP address	10.10.209.26
Netmask	255.255.255.0
Gateway	10.10.209.1
IP configuration	DHCP
DNS server 1	10.10.102.2
DNS server 2	10.10.102.3
SNMP Setting	
SNMP	● Enable ○ Disable
Community name	public
Contact	
Location	
IP Address report	
Auto report to IP	
Auto report to UDP port	0
Auto report period	10 seconds

10. Configure the following settings:
    a. IP Address
    Note that the IP address should be based on which network connection mask is being used. In "Step 13 of the CLC Static IP Address Configuration" the IP address used for the CLC was 10.1.1.1.

For this instance, set the IP address to the value 10.1.1.x where 'x' is any number between 2 and 254. The value of '1' cannot be used because the CLC was configured to that address. Any value used for subsequently configured CLCs should also not be used.

a. Netmask
   255.255.255.0
b. Gateway
   [leave blank]
c. IP Configuration
   Select **Static** from the dropdown.
d. DSN server 1 and server 2
   [leave blank]



Network Settings

IP address	10.1.1.10
Netmask	255.255.255.0
Gateway	
IP configuration	Static
DNS server 1	
DNS server 2	
SNMP Setting	
SNMP	● Enable ○ Disable
Community name	public
Contact	
Location	
IP Address report	
Auto report to IP	
Auto report to UDP port	0
Auto report period	10 seconds

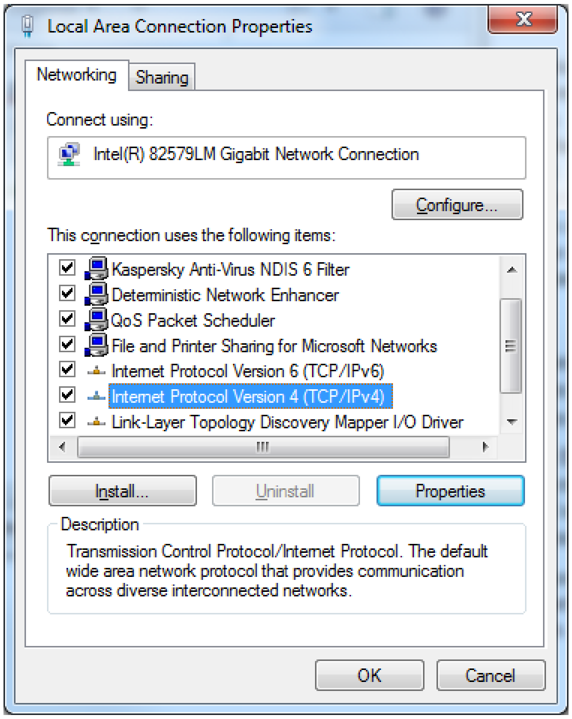
11. Write down the serial number of the APR-2 (or E2S-1) and the Static IP address used for your records.
12. Select **Submit**.
13. Select the **Save/Restart** link from the tree view on the left side of the webpage.

This completes the Static IP configuration process for the APR-2 (or E2S-1).

ACQUISITION COMPUTER STATIC IP ADDRESS CONFIGURATION

This section provides instructions on how to configure a computer with the Microsoft Windows 7 operating system to use a Static IP address.

1. Navigate to the **Control Panel**.
    a. Windows 7
        i. Select the **Windows Orb** (the **Start** button) and select **Control Panel**.
    b. Windows 10
        i. Enter **Control Panel** into the **Search Bar**.
        ii. Select **Control Panel** from the **Apps** list.
2. Select **Network and Sharing Center**.
3. Select the **Change adapter settings** link from the list on the left side of the page.
4. Select the Local Area Connection and then right-click to display the Right-click menu.
5. Select Properties.
6. Select Internet Protocol Version 4 (TCP/IPv4) as highlighted in the screenshot.



Connect using:

Intel(R) 82579LM Gigabit Network Connection

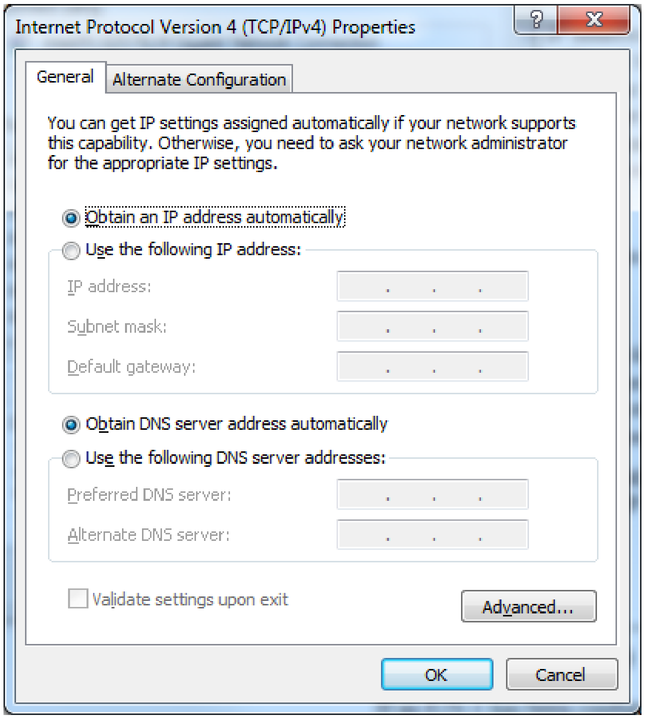
This connection uses the following items:

- ☑ Kaspersky Anti-Virus NDIS 6 Filter
- ☑ Deterministic Network Enhancer
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

7. Select Properties.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

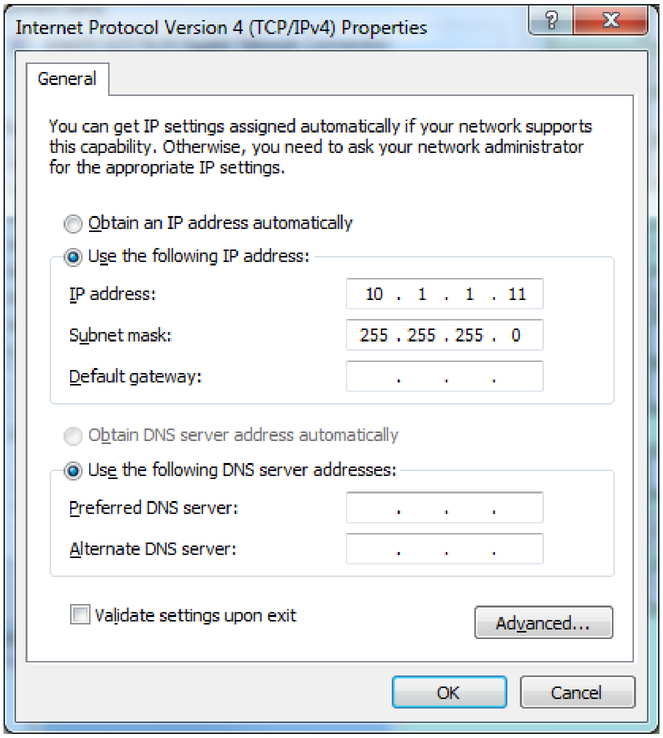
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

8. Select the radio button associated with *Use the following IP address*.
9. Configure the following settings:
    a. IP Address
       Note that the IP address should be based on which network connection mask is being used. In "Step 13 of the CLC Static IP Address Configuration" the IP address used for the CLC was 10.1.1.1. For this instance, set the IP address to the value 10.1.1.x where 'x' is any number between 2 and 254. The value of '1' cannot be used because the CLC was configured to that address. Any value used for subsequently configured CLCs should also not be used. The value of 10 should also not be used because the E2S-1 was configured to that address.
    b. Subnet mask
       255.255.255.0
    c. Default gateway
       [leave blank]



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 1 . 1 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

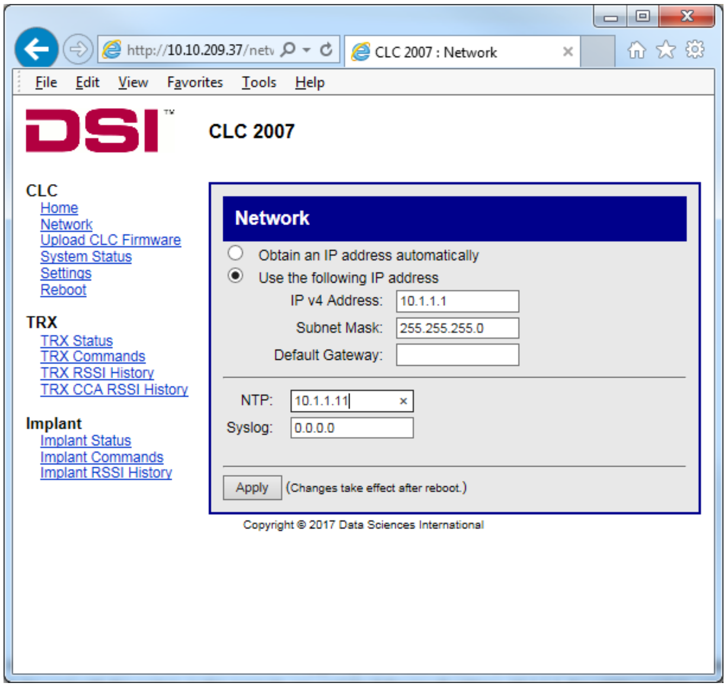
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

10. Write down the Static IP address used for your records. You will also need to enter this into the MX2/CLC Diagnostics' Network page for the NTP Server Address (see below).



http://10.10.209.37/netv

CLC 2007 : Network

CLC 2007

Network

○ Obtain an IP address automatically

● Use the following IP address

IP v4 Address: 10.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway:

NTP: 10.1.1.11

Syslog: 0.0.0.0

Apply (Changes take effect after reboot.)

Copyright © 2017 Data Sciences International

This completes the Static IP configuration process for the Acquisition Computer.

PONEMAH WORKSTATION BACKUP STRATEGY

This document points to areas where data is modified by the application and that data would need to be backed up on a regular basis.

TECHNOLOGY ESCROW

DSI recommends maintaining a copy of the installation media (e.g. DVD or an electronic copy of its contents) for all DSI software applications and service packs installed on the Ponemah workstation, should the workstation need to be rebuilt. Alternatively, a copy of the media may be requested from DSI and an electronic download will be provided.

Alternatively, DSI offers an annual agreement to become a beneficiary to DSI's account with National Software Escrow Inc. The escrow account is maintained by depositing all released versions of the software.

GOOD LABORATORY PRACTICE (GLP)

Enrolling as a beneficiary to DSI's escrow account is an excellent step to complying with FDA requirements for disaster recovery. As a beneficiary, the user is insuring their intellectual property in the event the property can no longer be supported.

BECOMING A BENEFICIARY

To become a beneficiary to DSI's escrow account, please contact a Ponemah representative. Enrollment as a beneficiary will be set up for the period of 1 year, upon which the user can renew their agreement each subsequent year. Upon purchase of the Escrow Agreement, you will receive written notification from National Software Escrow Inc. that you have been added as a beneficiary to DSI's escrow account.

NATIONAL SOFTWARE ESCROW, INC.

8225 Brecksville Road
Building Three, Suite 105
Brecksville, Ohio 44141
Phone: (440)546-9750
Fax: (440)546-9750
www.nationalsoftwareescrow.com

WHAT IS A TECHNOLOGY ESCROW?

Services provided by National Software Escrow, Inc. protect the interests of both technology developers (DSI) and their clients (DSI users) who license their products. Escrow beneficiaries rely on vendors for technical support and maintenance. This dependency, especially if it involves software related to mission-critical business operations, exposes them to certain risks. If, for instance, a technology vendor went out of business or stopped supporting the license software for other reasons, the licensee would likely suffer considerable losses in revenue and productivity. A technology escrow agreement gives licensees the ability, under specific and controlled circumstances, to gain access to the source code needed to maintain the technology.

PONEMAH DATA BACKUP

This section lists areas where data is modified by the Ponemah application. These areas should be backed up on a regular basis.

PONEMAH RUNTIME FOLDER

This folder is created upon installation of Ponemah. For versions 5.10 and newer, the default folder location is **C:\Ponemah**. If the user installs the application in a different folder, then all information below would be in that folder and sub-folders would be off the root folder. The following outlines the pertinent files that should be regularly backed up and the recommended backup frequency for each if the user changes their default configurations.

File	Description	Frequency of backup
AdvancedSearch_DefaultSearches.xml	This file contains the Searches available within Data Insight upon the initial loading of a Review (. RVW) file.	Anytime the file has been modified to update a default setting. If these files are not modified, the default settings will be available from the installation media.
TemplateTags.xml	This file contains the ECG PRO Template Tags available by from a Template graph by default upon the initial loading of a Review file.	
PPP3.INI	This file contains application and analysis attribute specific information that can be modified to update default settings.	

PONEMAH_DATA FOLDER

The default installation of the data folder is **C:\Ponemah_Data** for versions 5.10 and newer. If the user changes the default location during the installation process, the information will be under the user-specified location. The data folder contains all files created during an Acquisition and can be modified with a subsequent Replay or Review.

When using the *Study Protocol Option*, a subfolder is created within the data folder for each study. All files related to that study are placed in this subfolder.

The folder or study subfolder contains specific information for:

- .RAW (signal) data files
- .RVW review data files
- Derived data files
- Setup files
- Video files
- Signature files for electronic records
- Study Folders
- Video cameras configurations
- Templates

Folder or File	Description	Frequency of backup
C:\Ponemah_Data or default installation folder	This folder and subfolders contain all data files created during acquisition, replay and review.	Anytime an acquisition, replay or review has been performed, new data files will be created. The exception is a review session that has been performed but no marks sections have been saved.
..VideoCameras	This subfolder has the video camera configurations for the application. Each time a new video configuration is created these files are updated.	Only if video cameras are being used and anytime a new video camera configuration is created or when an existing camera configuration is modified.
..Templates	This subfolder contains templates that are used for the ECG PRO option.	Anytime a Template is created or modified.
Raw files (RAW), review files (RVW), video files (WMV, AVI), event files (EVT), Excel (xls, xlsb) or Access files (p3d) , signature files (SIG)	Whenever an acquisition is complete, at a minimum the RAW and RVW files will be created. Video files are only created if the video option is being used. If the user has ODBC as an output option, then one of the ODBC options (Excel or Access) will be generated. For the SIG files, these are only created or modified if using the Data Security Option.	Anytime an acquisition is performed new RAW, RVW and optional WMV files are generated. ODBC Excel and Access could also be generated. For Replay or Review, new ODBC data files will have been created. The review file can be modified.
Setup files (PRO, MDB, AMP)	The PRO file is the main setup file for the application. If OpenART is being used, an MDB file is generated containing the hardware configuration information. If an ACQ7700 or ACQ16 system is being used, an AMP file will be generated.	Anytime a setup (configuration) is created or modified.

PROGRAM AND FILES FOLDER

When the Ponemah application is installed, the installation also creates or updates the Microsoft SQL Server installation. Ponemah uses two instances of SQL Server, one for a production environment and one for a test environment which can be changed within the Ponemah application.

The Ponemah application itself creates a database within SQL Server and, for each study created through the Study Protocol Option, a database is created. Each one of these databases needs to be backed up on a regular basis, along with the system databases that are maintained in the same folder.

Depending on the version of Ponemah, different SQL Server Express versions were used. The following table outlines the versions of SQL Server used by Ponemah Version

SQL Server Version	SQL Server 2000 Desktop Edition	SQL Server Express 2005	SQL Server Express 2008 R2	SQL Server Express 2014
Ponemah Version	≤v4.80	v4.90-v5.10	v5.20	v5.30

It should be noted that Ponemah will detect and use any version of SQL Server that is installed on the workstation. If a Ponemah version upgrade is performed, Ponemah will use the currently installed version of SQL Server Express and not install any newer version. Only a clean install of Ponemah, without any version of SQL Server being on the workstation, will install the SQL Server versions listed above.

Refer to the table below for version specific information and the directory structure.

SQL Installation Folder and Database File Locations	Ponemah Version	Description
C:\Program Files\Microsoft SQL Server\MSSQL12.P3PLUS_V2	v5.30	This folder is for SQL Server 2008 Express and is used for the default P3Plus, production, instance of Ponemah. The folder contains all the database files that would be used by the application, as well as any system database files.
C:\Program Files\Microsoft SQL Server\MSSQL10.P3PLUS	v5.20	This folder is for SQL Server 2008 Express and is used for the default P3Plus, production, instance of Ponemah. The folder contains all the database files that would be used by the application, as well as any system database files.
C:\Program Files\Microsoft SQL Server\MSSQL10.P3PLUSTEST	v5.20	Same as above, except it is used for the P3PlusTest instance of the database. Typically, this is used for testing and the default P3Plus instance is used in production.
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data **Note:** This is for a new install of V4.90 only. Older version or an upgrade to v4.90 would use the SQL Server 2000 Desktop structure listed below.	v4.90-v5.10	This folder is for SQL Server 2005 Express and is used for the default P3Plus, production, instance of Ponemah. The folder contains all the database files that would be used by the application plus any system database files.
C:\Program Files\Microsoft SQL Server\MSSQL.2\MSSQL\Data **Note:** This is for a new install of V4.90 only. Older version or an upgrade to v4.90 would use the SQL Server 2000 Desktop structure listed below.	v4.90-v5.10	Same as above, except it would be used for the P3PlusTest instance of the database. Typically, this is used for testing and the default P3Plus instance is used in production.
C:\Program Files\Microsoft SQL Server\MSSQL$P3PLUS\Data	≤v4.80	This folder is for SQL Server 2000 Desktop (MSDE 2000) and is used for the default P3Plus, production, instance of Ponemah. The folder contains all the database files that would be used by the application plus any system database files.
C:\Program Files\Microsoft SQL Server\MSSQL$P3PLUSTEST\Data	≤v4.80	Same as above, except it would be used for the P3PlusTest instance of the database. Typically, this is used for testing and the default P3Plus instance is used in production.

Within the SQL Server Data folder, all database files are recommended to be backed up since the application and SQL Server database files are updated on a regular basis. Below is a simple script for SQL Server 2005 Express or SQL Server 2008 Express to perform that activity:

```
Net stop MSSQL$P3PLUS
xcopy  C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\*.* d:\backup
Net start MSSQL$P3PLUS
```

In the above example the destination location is **d:\backup** and should be replaced by the actual destination location, such as a network share.

Note: MSSQL.1 – This depends on the version of SQL Server being used. Select the correct path name from the SQL Installation Folder and Database File Locations table.

The frequency of backup depends on how often the application is used. For example, each time the application is started the Ponemah application database is always updated with the latest information such as the user who started the application.

For each Study database, the database is only updated when the user does study related activities, such as modifying a study, synchronizing Study related data, running acquisitions or doing a review of the data.

DSI REPORTING FOLDER

During installation, DSI Reporting is installed under the C:\Program Files(x86) directory in the **DSI Reporting** folder. The following outlines the pertinent folders that should be regularly backed up and the recommended backup frequency.

Folder or File	Description	Frequency of backup
DSI Reporting\Output	This subfolder is the default folder for the generated report.	Every time a report is saved in the default directory, if reports are maintained on the Ponemah workstation.
DSI Reporting\Templates	This subfolder is the default folder for the default report templates and any new templates that are defined.	Anytime a new template is defined or if an existing template is modified.

APPENDIX

The following instructions outline the necessary steps to update the Windows Settings per the recommended called out in this document.

POWER OPTIONS CONFIGURATION:

1. Select the **Windows Start menu | Control Panel.**
2. Change *View by* option in the upper right-hand corner from categories to **Small Icons.**
3. Select **Power Options.**
4. Select on (down arrow) for **Show additional plans**.
5. Select the radio button for **High Performance**.
6. Select **Change plan settings** link.
7. Select **Never** for the following settings:
    a. Dim the display
    b. Turn off the display
    c. Put the computer to sleep
8. Select **Change Advance Power Settings** link.
9. Expand the **Hard Disk**
10. Expand **Turn off hard disk after**
11. Change settings for both **on battery** and **plugged in** to **Never**
12. Expand **Sleep**
13. Expand **Sleep After**
14. Change settings for both **on battery** and **plugged in** to **Never**
15. Expand **Allow Hybrid Sleep**
16. Change settings for both **on battery** and **plugged in** to **Off**
17. Expand **Hibernate after**
18. Change settings for both **on battery** and **plugged in** to **Off**
19. Expand **USB Settings**
20. Expand **USB Selective Suspend Setting**
21. Change settings for both **on battery** and **plugged in** to **Disabled**
22. Expand **Power Buttons and Lid**
23. Expand **Lid Close Action**
24. Change settings for both **on battery** and **plugged in** to **Do Nothing**
25. Expand **Power Button Action**
26. Change settings for both **on battery** and **plugged in** to **Do Nothing**
27. Expand **Sleep Button action**
28. Change settings for both **on battery** and **plugged in** to **Do Nothing**
29. Expand **Processor Power Management**
30. Expand **Minimum Processor State**
31. Change settings for both **on battery** and **plugged in** to **100%**
32. Select **OK**.
33. Select **Save Changes**.
34. Close the window.

ENABLE NETWORK DISCOVERY

1. Navigate to the **Network and Sharing Center**.
2. Select **Change advanced sharing settings** from the list on the left.
3. Expand the desired network profile.
4. Enable the radio button for **Turn on network discovery**.
5. Click the **Save Changes** button.

ENABLE NO HIBERNATION

1. Navigate to the **Device Manager**.
2. Select **Disk Drives**.

3. Right-click the Disk Drive the software will be installed on and select **Properties**.
4. Select **Policies** tab.
5. Make sure both checkboxes have check marks.
6. Click **OK**.
7. Repeat for second drive
8. Close all windows.

ENABLE AUTOMATIC ADJUST CLOCK FOR DAYLIGHT SAVING TIME

1. Navigate to the **Date & Time.**
2. Select **Change time zone…** button.
3. Enable the check box for **Automatically adjust clock for Daylight Saving Time.**
4. Select **OK.**
5. Select **OK.**
6. Close the Control Panel.

DISABLE WINDOWS DEFENDER

Windows 7:

1. Select Windows Start Menu.
2. Right-click Computer and select Manage.
3. Select Services and Applications.
4. Select Services.
5. Navigate to and double-click **Windows Defender.**
6. Select the **Stop** button if the service is running.
7. Change the *Startup type* to **Disabled**.

Windows 10:

1. Disable Windows Defender Firewall
    a. Enter **Services** into the **Search Bar**.
    b. Select the **Services** desktop app.
    c. Right-click **Windows Defender Firewall** and select **Properties.**
    d. Select the **Stop** button if the service is running.
    e. Change Startup type to **Disabled.**
2. Windows Defender Antivirus Service
    a. Enter **Group Policy** into the **Search Bar**.
    b. Select the **Edit Group Policy** *Control Panel* option.
    c. Navigate to: **Computer Configuration | Administrativloce Templates | Windows Components | Windows Defender Antivirus**.
    d. Right-click **Turn off Windows Defender Antivirus** and select **Edit.**
    e. Select **Enable.**
3. Windows Defender Security Center Service
    a. Enter **regedit** into the **Search Bar**.
    b. Select the **regedit** *Run Command* option.
    c. Browse to: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\**
    d. Select **WinDefend** folder.
    e. Change **Start** from **2** to **4.**

DISABLE WINDOWS UPDATE

1. Navigate to the **Windows Update.**
2. Select **Change Settings.**
3. Select the drop down under **Important Updates** and select **Never Check for Updates.**
4. Select **OK.**
5. Close window.

DISABLE DEFRAGMENTATION (boot space optimizer)

1. Navigate to the **Performance Information and Tools**.
2. Select **Advanced tools** link.
3. Select **Open disk defragmenter** link.
4. Click **Configure schedule**.
5. Remove check mark on Run on a schedule (recommended).
6. Click **OK**.
7. Close all windows

DISABLE SEARCH INDEXING

1. Navigate to the **C:\** drive**.**
2. Right-click the **C:\** drive and select **Properties**.
3. From the **General** tab, uncheck **Allow files on this drive to have contents indexed**…
4. Select **OK.**
5. There will be an *Access Denied Error Message* screen, select **Continue**.
6. There will be an *Error Applying Attributes*, select **Ignore All**.
7. After the changes are complete, click **OK**.
8. Repeat the above steps for **D:** drive.
9. Close window.

DISABLE WINDOWS TIME AND WINDOWS SEARCH

1. Press <Ctrl>+<Alt>+<Delete>.
2. Select **Start Task Manager**.
3. Select the **Services** tab.
4. Select the **Services** button in the lower right corner.
5. Double-click **Windows Time.**
6. Change the *Startup type* to **Disabled**.
7. Select **OK**.
8. Double-click **Windows Search.**
9. Change the *Startup type* to **Disabled**.
10. Select **OK**.
11. Close all windows.

DISABLE THE FOLLOWING REGISTRY KEYS

1. Open a command window by clicking on the start button and typing "regedit" in the search window
2. Select the **regedit** program.
3. Disable Prefetcher
    a. Navigate to the following location: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters]
    b. Double-click **EnableSuperfetch**, change the **Set Value** to **0**, and select **OK**.
    c. Double-click **EnablePrefetcher**, change the **Set Value** to **0**, and select **OK**.
    d. Double-click **EnableBootTrace**, change the **Set Value** to **0**, and select **OK**.
4. Disable Boot Optimizer
    a. Navigate to the following location [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction]
    b. Double-click on **Enable**, change the **Set Value** to **N**, and select **OK**.
5. Disable NIC Card Power Settings (Green Mode) - *Lenovo computers*

   a. Navigate to the following location [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0007]
   b. If **PnPCapabilities** exist, set its value to 00000018

DISABLE AUTOMATIC UPDATES

1. Open a command window by clicking on the start button and typing “regedit” in the search window
2. Select the **regedit** program.
3. **Disable Adobe Updates**
   a. Navigate to the following location:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\11.0\FeatureLockDown]
   b. "bUpdater"=dword:00000000

4. **Disable Windows Update Notification**
   a. Navigate to the following location:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
   b. "DisableOSUpgrade"=dword:00000001

5. **Disable Office Updates**
   a. Navigate to the following location:
   [HKEY_LOCAL_MACHINE\software\policies\microsoft\office\16.0\common\OfficeUpdate]
   b. "EnableAutomaticUpdates"=dword:00000000
   c. "HideEnableDisableUpdates"=dword:00000000

6. **Hide Warning Flag**
   a. Navigate to the following location:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]
   b. "HideSCAHealth"=dword:00000001

7. **Disable Windows 10 upgrade**
   a. Navigate to the following location:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows]
   b. "DisableGwx"=dword:00000001

8. **Disable Windows 10 upgrade message**
   a. Navigate to the following location:
   [[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GWX]
   b. "DisableGWX"=dword:00000001

OPENING FIREWALL PORTS

Windows 7 and Windows 10

1. Navigate to the **Control Panel**.
2. Select **Windows Firewall.**
3. Select the **Advanced settings** link on the left**.**
4. Select **Inbound Rules** from the left pane.
5. Right-click Inbound Rules and select **New Rule**.
6. Select the **Port** radio button and click **Next**.
7. Select the protocol (**TCP** or **UDP**) and enter the port number into the text field associated with *Specific local ports*, then click **Next**.
8. Select **Allow the connection** and then click **Next**.
9. Select the **Domain** and **Private** for the *Network Type* to which this port rule applies, then click **Next**.
10. Enter a meaningful **Name** for the rule and an optional **Description**, then click **Finish**.