WORKSTATION CONFIGURATION GUIDE



This document addresses the steps required to achieve 21 CFR part 11 compliance when setting up and enVigil Server Workstation. Steps are also taken to disable features of the Operating System that could cause issues and prevent the system from continuous operation.

Introduction

This document constitutes a step by step procedure to be used when implementing a monitoring system based on enVigil Facility Monitoring Software. It concentrates on PCs running Windows XP Professional SP2/SP3 and Windows 7 Ultimate or Professional addition. enVigil only supports 32 bit versions of these operating systems. Windows Vista is supported by enVigil, due to its similarity to Windows 7. The Windows 7 steps of this document can be used to configure Windows Vista and although there may be some slight differences, the steps contain enough information to apply the equivalent changes.

This document lists the steps necessary when installing and configuring *enVigil 3.0* as a stand-alone system on a brand new PC's Windows installation.

Additional steps are required when implementing an enVigil view node system and are covered in a separate document *enVigil Remote Client Configuration Procedure* that document addresses both the changes needed on the enVigil Server PC and the enVigil Client installation procedure on the remote client.

For computers intended to run as a part of a domain you should be aware that any configuration changes made prior to joining the computer to the domain may be reset by the domains group policy. Therefore you should always check each step of this document after the computer has been joined to the domain.

PC Prerequisites

Most enVigil implementations will use a new computer where the OS is pre-installed but not completed.

The PC specification will vary between projects, however several requirements are common:

- The OS should be Windows XP Professional SP2/SP3 or Windows 7/Vista (Ultimate or Professional).
- A Network Interface must be fitted (even if the PC will not be networked).
- A Parallel Port or spare USB port must be fitted to accommodate the security key (dongle).
- Spare PCI slot(s) should be available if serial interfaces are to be used.
- A USB Port should be fitted for printer support.
- An internal speaker should be fitted.
- All disks should be formatted as NTFS.
- A second, identical hard disk is recommended, for 'ghosting' or backup.
- A CD Writer is recommended.

Turning on the Computer for the First Time – Windows XP

When turning on a new computer for the first time it will complete the setup of Windows by presenting a series of screens and dialog boxes.

It may be that the PC comes with the operating system preloaded in which case you can skip this section and go to the **'Configuring the PC'** section.

Accept any PC manufacturer's license agreements as necessary and wait until the 'How should dates and currency appear?' is shown. Select the appropriate country settings and click 'Next':

Accept Microsoft's license agreements as necessary and proceed to the 'Help protect your PC' screen.

Select 'Not right now' in answer to the turn on automatic updates question.

Entering the PC's name and description

You are now required to enter the PC name and description:

The 'Computer name' will have been specified in the project 'Functional Design Specification' (FDS) or 'Software Design Specification' (SDS) and will typically be 'EMS-Server' or 'FMS-Server'. DO NOT USE UNDERSCORE CHARACTERS; instead use the 'minus' character.

The computer description should be used to help describe the PC's function e.g. 'PharmaQual EMS Server'.

Entering the Administrator password

The 'Administrator password' is critical and should be set to '*Administrator'* at this stage. It is likely that the customer or end-user will take ownership of the main Administrator account at a later stage.



Windows**

Selecting the Internet Connection Method

The next screens concern the internet connection method, and should be set to `LAN'.

If the PC is not part of a network with a DHCP server, and if you do not know the relevant IP addresses, then skip the screen that asks you to fill them in.

Registering with Microsoft

The next Windows setup screen concerns registering with Microsoft and should be set to 'No, not at this time':

Creating the initial user account as 'emsuser'

When asked to provide your name (and up to 4 other user's names), enter 'emsuser' as 'Your name' and leave the rest blank – this will create the initial 'emsuser' account at administrative level:



Dell'

On completion of the Windows XP installation, the PC will eventually reboot and present a familiar Windows XP desktop.



Turning on the Computer for the First Time – Windows 7

You must install either Windows 7 Ultimate (32 Bit) or Windows 7 Professional (32 Bit). enVigil does not support 64 Bit versions of the operating system.

Prior to installation ensure the PC is not connected to any network.



Even if performing an upgrade from another version of Windows select the 'Custom (advanced)' option. This ensures a 'clean' installation.

Select the disk or disk partition that you wish to install Windows 7 on and click the 'Next' button:

Windows will begin the first major phase of installation and can take many minutes to complete:

The Windows 7 installer will then reboot and you should see the 'Starting Windows' screen. It will be followed with some other screens labelled 'Updating registry settings..' and 'Setup is starting services...':



After a few minutes you should see the 'Completing installation' screen:



The installer then reboots the system for the second time:



You are now required to enter the default user account and computer name:

Use '**emsuser**' as the default user name.

The 'computer name' will have been specified in the project 'Functional Design Specification' (FDS) or 'Software Design Specification' (SDS) and will typically be 'EMS-Server' or 'FMS-Server'. DO NOT USE UNDERSCORE CHARACTERS; instead use the 'minus' character.

Enter and confirm the password as 'emsuser'. A password hint so enter a password hint of 'EMS User standard':





When prompted carefully enter the product key. You can usually find the product key on the installation case. Ensure that the 'Automatically activate Windows when I'm online' check box is unchecked:

You may at this stage be taken to the 'Help protect your computer and improve Windows automatically' screen. Select the 'Ask me later' option:

Set the system clock as required. Ensure that the clock is set to automatically adjust for Daylight Saving Time :

Windows 7 installer will then begin to prepare the desktop:





The Windows 7 desktop will then be shown:



Windows 7 Installation is complete!

Configuring the PC

The following section describes the configuration of 'environmental' parameters required for optimum performance with enVigil. Examples are shown for Windows XP and the equivalent steps taken for Windows 7.

Setting up the Control Panel

• In Windows XP the control panel should be set to '*Switch to Classic View'* to enable all options to be accessed:

E' Control Panel Ele Edit Wow Favettes Tools Help Control Favettes Tools Help Folders Control Favet	2 - C X 27 2 - C X	Control Panel Fle Edit View Favorities Tools One A - O - D - D - O - O - O - O - O - O - O	Help sarch 论 Fol	ders .					
Control face Indust types In	Pointers and Other Handware Image: Constant State Image: Constant State	Constant Frankt	Accessibility Options Depkry Keyboard Regional and Language	Add Hardware Folder Options Mouse Scamers and Comers as User Accounts	Add or Remov Feets Network Convertions Schwähed Teks Windows Fremai	Adjanctivative Took Game Controllers Controllers Waard Network Setup Security Center Waters Network Setup Security Center	Automatic Updates Enter(II), GHA Driver Phone and Modem Sounds and Audo Devices	Prover Options Speech	Data and Time Data and Time Jana Ray II Partiest and Partiest and System

• In Windows 7 ensure 'View by:' is set to either 'Small Icons' or 'Large Icons':

Jo iger control parties a	• • • Search Control Pane?	Control Panel + All Co	ntrol Panel Itema 🕨	Search Control Panel
Adjust your computer's settings	View byl Category *	Adjust your computer's settings		View by Small icons -
 Before your computer's share and your computer's share and the first post computer that and fix post computer with the post of the post o	Order Products Charge account type Appearance and Personalization Charge the there Charge the there Charge the there Charge the there Charge account of the input methods Charge texplored or other input Charge texplored or other input methods	 Action Cetter Eactury and Rentere Decise Manager Ensise Manager Ensise Manager Ensise Manager Ensise Manager Internet Options Misuse Prover Options Prover Options Prover Options Speech Recognition Speech Recognition Testeba and Stoct Menu Vindows Regime Windows Filewall 	California and Amagement California and Printeen California and Printeen California and Printeen California and Printeen California	Intelligence Credential Manager Restrop Grägets Restrop Grägets Brand Intering Optime Destination and Other Sensors Intering Optime Those and Modern Restrop Grägets Processor and Modern Sound System User Accounts Mindows Defender

Removing unwanted applications

It is now necessary to remove undesirable applications such as trial versions of Anti-Virus or Dell OpenManage Client Instrumentation (OMCI). Attempt to shut down and disable any Anti-Virus and non-Microsoft Firewalls then use the Control Panel .. Add/Remove Programs to locate and uninstall these programs. Note that there may be several additional components such as 'LiveUpdate', 'LiveReg' etc. that must also be uninstalled.

It is difficult to define the unwanted applications as the software installed on each PC is likely to change frequently. You should make a valued judgement as to whether the software is really needed. If you have any concerns or questions you should consult your IT department.

For Dell machines ensure that Dell OMCI if present is uninstalled before proceeding.

Ensure that any unwanted entries are also removed from system startup (such as the 'EULA Launcher' on Dell machines). To run the system startup setup..

XP: Perform Start-> Run->msconfig.

Windows 7: Simply type 'msconfig' in the start menus search bar and hit the enter key. Uncheck any unused applications.

eneral SYSTEM.INI WIN	I.INI BOOT.INI Services Startup	
Startup Item	Command	Location
QTTask Green CueC52Tray Acrotray Crotray Crotray QTTask Scheduler Ache Campa	"C:IProgram Files/QuckTime()TTask.exe" at "C:IProgram Files/JTunes/Ielper.exe" "C:IProgram Files/JAdbe/JAdbe Version Cue "C:IProgram Files/JAdbe/JAcobe 8.0/JAcrobet C:IVIDDOWS/system32/ctfmon.exe "C:IProgram Files/QuckTime(QTTask.exe" at scheduler -UDDoctDate.IS/COMMON_UL/Schulton IPP	HKLM/SOFTWARE/Microsof HKLM/SOFTWARE/Microsof HKLM/SOFTWARE/Microsof HKLM/SOFTWARE/Microsof HKCU/SOFTWARE/Microsof HKCU/SOFTWARE/Microsof HKCU/SOFTWARE/Microsof
HP Digital Imaging	C:\PROGRA~1\HP\DIGITA~1\bin\hpdtra08.exe	Common Startup
HP Photosmart Pre	C:\PROGRA~1\HP\DIGITA~1\bin\hpqthb08.e	Common Startup
<		
	Enable All	Disable All

Setting the display resolution and blank screen saver

Windows XP:

- 'Display Properties .. Settings .. Screen resolution' should be set to 1280 x 1024 as a minimum resolution:
- 'Display Properties .. Screen Saver .. Screen saver' should be set to 'Blank' with 'On resume, password protect' unchecked:



Setting the display resolution and blank screen saver (cont...)

Windows 7:

- Right click the Desktop and select 'Screen resolution'. Adjust the slider control to set the screen resolution to at least 1280 x 1024
- Right click the Desktop and select 'Personalize' from the pop up menu. Click the 'Screen Saver' button located at the bottom right corner of the Personalization dialog box. *Screen saver* should be set to '*Blank'* with '*On resume, display logon screen'* unchecked:

Change the appearance of your display	Screen Saver
Display: 1.0ELL1X07FV Resolution: 2280 × 1024 (recommended) Orientation: High Main text and other High Whot digplay settor Advanced settings EE0 × 500 Low:	Screen saver Blank Settings Preyiew Wait 1 minutes On resume, display logon screen Power management Conserve energy or maximize performance by adjusting display brightness and other power settings. Change power settings

Setting a basic theme - (Windows 7 only)

• Right click desktop and select 'Personalize' from the pop up menu. Scroll down to 'Basic and High Contrast Themes' select either 'Windows Classic' or 'Windows 7 Basic':



Disabling the Welcome screen and setting 'emsuser' password (XP only)

- The Welcome screen should be disabled (and therefore fast switching between users): 'Control Panel .. User Accounts .. Change the way users log on or off' should be set to not use the Welcome screen:
- Use the User Accounts screen to set the 'emsuser' user password to 'emsuser'



Setting up Windows 7 Logon screen (Windows 7 Only)

• Run the 'Local Group Policy Editor' by typing 'gpedit.msc' in the start menus search bar. Under *Local Policy->Administrative Templates->System->Logon* ensure 'Hide entry points for Fast User Switching' and 'Always use classic logon' settings are enabled

Local Group Policy Editor				
<u>File Action View H</u> elp				
🗢 🔿 🙋 🖬 🔒 🚺 🖬 🛛 🍸				
Local Computer Policy Computer Configuration Software Settings Mindows Settings Administrative Templates Control Panel Network Printers System Credentials Delegation Device Installation Device Redirection Disk NV Cache Disk Quotas Distributed COM Driver Installation Dister CodentialsIngle	H	Setting Setting Setting Setclude credential providers Do not process the legacy run list Turn off Windows Startup Sound Hide entry points for Fast User Switching Always use classic logon Nun these programs at user logon Always wait for the network at computer startup and logon Always use custom logon background	State Not configured Not configured Not configured Enabled Enabled Not configured Not configured Not configured Not configured	Comment No No No No No No No No No No No
 ▷ Filesystem ○ Folder Redirection ○ Group Policy ▷ ○ Internet Communication Mana ▷ ○ SCSI 	+	Extended), Standard /		
11 setting(s)				

Setting the Administrator password (Windows 7 Only)

 By default the built in Administrator account is hidden after Windows 7 installation. It should be enabled and set up with a suitably secure password.

Set the password via Control Panel ->Administrative Tools->Computer Management->System Tools->Local Users and Groups->Users. Right click the 'Administrator' user and select the 'Set Password...' option.



Disabling the Windows Firewall (Windows XP)

• 'Control Panel .. Windows Firewall .. General' firewall protection should be switched off:

If it is not possible to turn off the firewall or an external non-Windows firewall is protecting the system (e.g. enforced by customer) you must:

From the 'Exceptions' Tab 1) Click 'Add Program...' 2) Use 'Browse' button to navigate to the enVigil Installation directory and select and add the Launch. exe Program. Repeat to also add DBXServer.exe 3) Click the 'Add Port...' button. Set the 'Name' field to 'DCOM' and set the port number to 135, ensuring the 'TCP' radio button is selected and then click OK.

ws Firewall
Exceptions Advanced
Windows Firewall is helping to protect your PC
vs Firewall helps protect your computer by preventing unauthorized users ining access to your computer through the Internet or a network.
C On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions ta
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Window Firewall blocks programs. Selections on the Exceptions tab will b ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
vs Firewall is using your domain settings.

ws Firewall		\mathbf{X}	Add a Dort			
Ecoptions Advanced			AUU a Port			
In Farwall is blocking incoming network and services released below. Adding better but might increase your security is and Services.	k connections, except for the g exceptions allows come programs risk.		Use these settings number and protoc want to use.	to open a port ol, consult the i	through Windows Firewall. To find the p documentation for the program or servic	ort e you
	Broup Policy					
obe Veroion Due DS2	No					
and Printer Shaing	Yes					
UNCHEXE	No			DCOM		
naged Services Agent	No		<u>N</u> ame:	DCOM		-
er Heniote Assistance	Tes					
er Henote Admitance - Port	Tes			1.05		
rece Automatics	THE .		Port number:	135		
mote Nativitation - windows messent				L		
naviec Anthins	No					
P Farmanet	Rin N			TCP		
Pogram. Add Pgrt.	Edt Delete			<u> </u>	○ <u>⊥</u> .	
leg e gotiñ cañon when Windows Fiew	all blocks a program		What are the risks	of opening a po	ort?	
	OK Cance		Change scope)	OK Cano	el

Window program to work

Nam

Add Disp What

Disabling the Windows Firewall (Windows 7)

• `Control Panel .. Windows Firewall ...Click Turn Windows Firewall on or off. ...Click Turn off Windows Firewall (not recommended) under each network location, and then click OK:



If it is not possible to turn off the firewall or an external non-Windows firewall is protecting the system (e.g. enforced by customer) you must add 'Inbound' and 'Outbound' rules for the DBXServer.exe and Launch.exe applications and also DCOM port 135.

To add a program... (For both DBXServer.exe and Launch.exe in turn)

Click 'Advanced settings' from the Windows Firewall screen 1) Select 'Inbound Rules' from the left pane and click 'New Rule...' from the

action pane to the right of the screen

2) Leave 'Program' selected and click the 'Next>' button

3) Ensure 'This program path:' is selected and use the 'Browse...' button to locate and select the application from the enVigil installation directory and then click 'Next>'

4) Ensure 'Allow the connection' is selected and click 'Next>'

5) Ensure that all check boxes are enabled for 'Domain', 'Private' and 'Public' and click 'Next>'

6) Enter a suitable name of 'DBXServer' and 'Launch', you can leave the description blank.

REPEAT STEPS 1-6 but use 'Outbound Rules' in step 1.

DCOM Port 135 Rule...

7) Select 'Inbound Rules' from the left pane and click 'New Rule...' from the action pane to the right of the screen

8) Select 'Port' instead of 'Program' and click the 'Next>' button

9) Ensure TCP is selected and enter `135' in the `Specific local ports:' field and click the `Next>' button

10) Ensure 'Allow the connection' is selected and click 'Next>'

11) Ensure that all check boxes are enabled for 'Domain', 'Private' and 'Public' and click 'Next>'

12) Enter a name of 'DCOM', you can leave the description blank. **REPEAT STEPS 7-12 but use 'Outbound Rules' in step 7.**

Windows Firewall with Advanced	Security					
<u>File Action View H</u> elp						
🗢 🄿 🖄 📰 🔜 🔹						
Windows Firewall with Advance	Inbound Rules					
Inbound Rules	Name	Group	Profile	Enabled	Action	-
Connection Security Rules	Zaunch		All	Yes	Allow	
Monitoring	OBXServer		All	Yes	Allow	=
	O DCOM		All	Yes	Allow	

Disabling Windows Defender (Windows 7 Only)

 `Control Panel .. Windows Defender ...Tools...Options...Administrator.. Ensure `Use this program' is unchecked and click the `Save' button

NOTE: Windows Defender may not be able to be disabled until it is updated via the internet. If possible you should temporarily connect the PC to the internet to update defender. Once updated it can be disabled.



Disabling Security Alerts and Automatic Updates(Windows XP)

 'Control Panel .. Security Centre' alerts should be disabled for Firewall, Automatic Updates and Virus Protection:



Disabling Security Alerts and Automatic Updates(Windows 7)

• *`Control Panel .. Action Center...Change Action Center Settings...* Ensure all check boxes are unchecked and click the *`OK'* button:

	View Tools Help	Edit View	e
	Turn messages on or off		
for problems and send you a message if problems are found. <u>s?</u>	For each selected item, Windows will chee How does Action Center check for proble		
	Security messages		
Spyware and related protection	Windows Update		
User Account Control	Internet security settings		
Virus protection	Network firewall		
	Maintenance messages		
Check for updates	Windows Backup		
	Windows Troubleshooting		
	Related settings		
gram settings	Customer Experience Improvement Pr		
	Problem reporting settings		
	Windows Update settings		

• 'Control Panel .. Windows Update... Change Settings'. Ensure 'Never check for updates(not recommended)' is selected for 'Important updates'. Ensure check boxes under 'Recommended updates' and 'Who can install updates' are also unchecked and click the 'OK' button:

<u> </u>	
	Choose how Windows can install updates
	When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.
	How does automatic updating help me?
	Important updates
	Never check for updates (not recommended)
	Install <u>n</u> ew updates: Every day v at 03:00 v
	Recommended updates
	Give me recommended updates the same way I receive important updates
	Who can install updates
	Allow all users to install updates on this computer
	Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Setting Local Security Policy (server only Windows XP & Windows 7)

• 'Control Panel .. Administrative Tools .. Local Security Policy.. Local Policies .. Security Options .. Network access: Sharing and security model for local accounts' should be set to 'Classic – local users authenticate as themselves' to allow Sharing and Security to be configured:



Installing enVigil

After the first user account has been setup and the initial boot sequence is complete the computer is ready for the installation of enVigil. To install enVigil you must ensure that you are logged in as a user that has full local administrative privileges.

If you are installing on a Windows 7 machine it is recommended that 'User Account Control' is turned off prior to installation. If it is not switched off the enVigil Installer will be unable to create the default local user accounts and these will have to be added manually.

User Aco Tail root in	ount Control In	elps prevent potentially harmful programs from making changes to your c kccount Control settings	computer.
iles,	o metily		
-	1 -	Never notify me where	
		Programe by to install self-wate or make changes to	
-	-	English changes to Windows atting	
-			
		() Not examined the only if you need to	
-6		son programs that are real seriilized for Windows 7 Instance they do not support User Assessed Control.	
Mare	notify		

Turn off UAC at following location '*Control Panel .. User* Accounts ..Change User Account Control settings..'. Move the slider down to 'Never notify' and click the OK button. Reboot the PC to enable the UAC setting change.

€√	Welcome to the InstallShield Wizard for enVigil FMS Version 3
envigil	The InstallShield(R) Witzerd will install en/ligil FMS Version 3 on your computer. To continue, click Next.
	WWRIGHS: The program is protected by copyright law and international treaters.
	< gack Next > Cancel
🖗 enVigil FMS Version :	8 - InstallShield Wizard
Destination Folder Click Next to install to I	his folder, or click Change to install to a different folder.
Install en/lig	IFMS Version 3 to:

< Back Next > Cancel

< Back Next > Cancel

tup Type

B enVigil FMS Version 3 - InstallShield Wizard

Help Space < Back Next >

en/igil Clent
 en/igil Server

e

Insert the enVigil installation CD and the setup process should auto-run. If it does not, then navigate to the CD drive and run the enVigil Windows Installer package (for example, enVigil FMS Version 3.msi) located there and follow the on-screen installation instructions:

It is recommended that you accept the default installation folder of `C:\Program Files\Pharmagraph\enVigil'. If required you can install to a different directory.

If installing on Windows 64 bit the default directory will be 'C:\Program Files (x86)\Pharmagraph\enVigil'

enVigil allows you perform a 'Custom' installation which allows you to specifiy whether to install 'enVigil Client', 'enVigil Server' and 'Demonstration configuration components'.

For machines that will run as an enVigil Server it is always recommended to choose the complete installation option.

1.	Select the program features you want installed.	en en
	Click on an icon in the list below to change how a feature is insta	lled. Feature Description
	Image: This feature will be installed on local hard dr Image: This feature, and all subfeatures, will be installed Image: This feature will be installed when required. Image: This feature will not be available.	ive. Illed on local hard drive.
]	Install to: C:VProgram Ries/Pharmegraph/en/lg/l,	Chenge

If the enVigil Client software is really not required then you should select 'Custom' click the 'Next'button, select the 'This feature will not be available' option under the 'enVigil Client ' feature and click the 'Next' button.



Installation is then ready to begin. Click the 'Install' button to start the installation.

During installation a progress bar will be shown while various tasks are being performed. Installation may take serveral minutes to complete.

Note: If installing on Windows 7 with User Account Control turned on you will be prompted to authorise the installation at various times. These security prompts suspend the installation.

The installer should show this screen when complete. Click the 'Finish' button.

When enVigil has been installed successfully some desktop shortcuts will have been created;

'Configure enVigil Server' - can be used to run the enVigil Server configuration program. It will only been created if the enVigil Server feature was chosen to be installed (or the 'Complete' installation option was chosen).

'enVigil Client Demonstration' - will run the enVigil Client software. If the 'Demonstration configuration' was chosen to be installed (or the 'Complete' installation option was chosen) the PharmaQual enVigil Demonstration client VCX file wil be run. If the demonstration config was not chosen to be installed then enVigil client will run with a new (blank) screen ready for configuration. This shortcut will not be created if the enVigil Client feature was chosen to not be installed.

'Example PlayWave' - can be configured to play an audible alert when some system event occurs (please refer to the PlayWave manual section of the *enVigil-FMS System Configuration Guide*).





enVigil Client Demonstra...



Local User Accounts

The *enVigil* installation process should have created the following additional local user accounts:

Account name	Password	Information
EMSadmin	<predefined by="" pharmagraph=""></predefined>	Reserved administrator account for system maintainence
EMSsystem	<predefined by="" pharmagraph=""></predefined>	Reserved administrator account used to run background server processes
Manager	Manager	Administrator account used to create example enVigil 'Manager'
Supervisor	Supervisor	Standard User account used to create example enVigil 'Supervisor'
Operator	Operator	Administrator account used to create example enVigil 'Operator'

If installation was carried out on Windows 7 while 'User Account Control' was turned on the installer would have failed to create these user accounts. The 'EMSuser', 'EMSsystem' and 'EMSadmin' accounts should therefore be added manually.

For non-Pharmagraph systems you can reset the EMSsystem and EMSadmin passwords. Be sure to document and safeguard the modified passwords.

Setting the default Password Policy (Windows XP & Windows 7)

• 'Control Panel .. Administrative Tools .. Local Security Policy.. Security Settings.. Account Policies.. Pasword Policy\Account Lockout Policy' Apply the following settings:

Policy	Setting
Enforce Password History	0 passwords remembered
Maximum Password Age	0 Days
Minimum Password Age	0 Days
Minimum Password Length	6 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled
Account lockout duration	0 (Admin Reset)
Account lockout threshold	3 invalid logon attempts
Reset account lockout after	3 minutes

The enVigil Server service will now be setup to run under the 'EMSsystem' account.

Running the enVigil Server service as the 'EMSsystem' account (server only) (XP & Windows 7)

If the demonstration configuration has not been installed this step can only be carried out once the enVigil Server has been configured to run at least one process.

- 'Control Panel .. Administrative Tools
- .. Services .. enVigil Server .. Properties
- .. Log On' should be set to 'This account' '.\emssystem' with the appropriate
- password entered and confirmed:

"le Action View	Help					
- → 🗷 🗗						
g Services (Local)	Services (Local)					
	en/ligil Server	Concerter December	Maintains a	enVigil Server Prope	rties (Local Computer)	2
	Stop the service Restart the service	Cryptographic Servi	Provides th.	General Log On Rec	overy Dependencies	
		BOHCP Chent	Nanages rs	Log on as:		
ත්වය ක්ෂය මූහ		Cistributed Link Tra	Solishibuted Link Tra Maintains II Coordinate Coordinate Coordinate			
		CNS Client	Resolves a	Allow cervice to	interact with desktop	
		SengineServer Serving Security	McAfee En Authentice	This account	encycles	Browos.
		Reenvigi Server		Pasoword		
		School Reporting Ser	Allows erro Enables ev	Conlinn password		
		SPast User Switching SpFax	Provides m Enables you	You can enable or doa	ble this service for the hardware	prolies listed below.
		PLEXnet Licensing 5	This servic	Hardware Profile		Service
	\ Extended & Standard /			Ptofile 1		Enabled



If the service is currently running then you may get a warning to stop and restart the service. This can be easy achieved using the 'restart' icon



Checking local accounts for password expiry (XP & Windows 7)

Now check that the 'EMSsystem', 'EMSadmin' and 'EMSuser' user accounts are set to never expire.

Description: enVigil	system
User must change passwo	ord at next logon
User cannot change pass	word
Password never expires	
Account is disa <u>b</u> led	
Account is locked out	

• 'Control Panel .. Administrative Tools .. Computer Management .. Local Users and Groups .. Users' the properties of each of those user's accounts should look like this:

Creating Task Bar Shortcuts(server only) (XP & Windows 7)

Because 'emsuser' will eventually be a low privilege account, some task bar shortcuts should be added. This is handled slightly differently in Windows XP and Windows 7. In Windows XP shortcuts are added to the 'Quick Launch' toolbar, Windows 7 allows you to 'pin' items to the taskbar.

Shortcuts will be created on the task bar so that certain facilities can be run using a higher privilege account such as 'EMSadmin'. Three new shortcuts will provide convenient access to the 'Local User Manager' Windows MMC 'plug-in', the 'Configure enVigil Server' (ConfServer.exe) program and the 'Configure enVigil Users' (ConfUserAcess.exe) program.

Windows XP: If the 'Quick Launch' toolbar is not visible, right click the task bar at the bottom of the screen and select 'Toolbars'..'Quick Launch':

askbar	Start Menu
- Taskb	ar appearance
2	Start 🖉 🦉 🝳 🔁 2 Internet 🛅 Folde
<mark>.</mark> ∎o	ck the taskbar
Au	to-hide the taskbar
🗹 Ke	ep the <u>t</u> askbar on top of other windows
🗹 <u>G</u> r	oup similar taskbar buttons
Sh Sh	ow <u>Q</u> uick Launch
Notific	ation area
	🔇 🚅 🌫 1:23 PM
🗹 Sh	ow the cloc <u>k</u>
You c have	an keep the notification area uncluttered by hiding icons that you not clicked recently.

Figure 1: Enabling the Quick Launch Toolbar (XP Only)

Windows 7 does not have the 'Quick Launch' facility but instead you can simply 'pin' items to the task bar. To pin an item to the task bar simply drag the item (shortcut to application) to the task bar and release.

Adding a Task Bar Shortcut to Local User Manager (server only) (XP & Windows 7)

To create the 'Local User Manager' shortcut, navigate to the 'C:\Windows\System32' folder, right click on 'LUSRMGR.MSC' and select 'Send to'>'Desktop(create shortcut)'. Right click the resulting shortcut added to the desktop to access its properties:

Shortcut to lu	ısrmgr.msc Properties 🔹 💽 🔀	Shortcut to lusrmgr.msc Properties ? 🛛
General Shor	tcut Security	General Shortcut Security
\$	Shortcut to lusrmgr.msc	Shortcut to lusrmgr.msc
Type of file: Opens with:	Shortcut	Target type: Microsoft Common Console Document Target location: system32
Location: Size:	C:\Documents and Settings\Administrator.asl\Applic	Target: C.W/INDOWS\system32\lusrmgr.msc
Size on disk:	4.00 KB (4,096 bytes)	Shortcut key: None
Created:	11 November 2010, 11:58:20	<u>R</u> un: Normal window
Modified:	11 November 2010, 11:58:20	Comment:
Accessed:	12 November 2010, 10:47:57	Eind Target Change Icon Advanced
Attributes:	Read-only Hidden Advanced	
	OK Cancel Apply	OK Cancel Apply

Figure 2: Local User Manager Shortcut (Windows XP)

On the '*General'* tab set the shortcut name to be 'Manage Windows Users' – this then appears as the tool tip when the user hovers over the Quick Launch icon.

On the 'Shortcut' tab, click the 'Advanced...' button

Windows XP: ensure that the '*Run with different credentials'* check box is checked then click OK:

Windows 7: ensure that the '*Run as administrator'* check box is checked then click OK:

Windows XP: Hold down the shift key and drag the shortcut from the desktop to the Quick Launch toolbar to the right of the Start button.

Windows 7: Simply drag the shortcut to the task bar, position it to the right of the Start button if possible.

You can delete the shortcurt that was originally added to the desktop.

Adding a Task Bar Shortcut to Configure enVigil Server (server only) (XP & Windows 7)

The existing desktop shortcut to 'Configure enVigil Server' should now have its advanced properties set as'*Run with different credentials'(Windows XP Only), 'Run as Administrator' is not required for Windows 7.* Close the properties dialog then drag the shortcut to the Quick Launch toolbar(Windows XP) or Pin the shortcut to the task bar (Windows 7).

Configure enVi	gil Server Properties 🛛 🛛 🛛 🔀
General Shortc	ut Compatibility Security
si Sing Co	onfigure en Vigil Server
Target type:	Application
Target location:	enVigil
<u>I</u> arget:	gram Files\Pharmagraph\enVigil\ConfServer.exe"
<u>S</u> tart in:	"C:\Program Files\Pharmagraph\enVigil\"
Shortcut <u>k</u> ey:	None
<u>B</u> un:	Normal window
Comment:	Configures enVigil Server
Eind	Target Change Icon Agvanced

Figure 3: Configure enVigil Server Shortcut (Windows XP)

Adding a Task Bar Shortcut to Configure enVigil Users (server only) (XP & Windows 7)

A shortcut to 'Configure enVigil Users' should now be added by navigating to the enVigil folder ,'ConfUserAccess.exe' application, right clicking it and selecting 'Send to>Desktop(create shortcut)', then using the same technique described above to set its advanced properties. Close the properties dialog then drag the shortcut to the Quick Launch toolbar(Windows XP) or Pin the shortcut to the task bar (Windows 7).

hortcut to Co	nfUserAccess.exe Properties 🛛 🔹 🔀
General Shortc	ut Compatibility Security
윩 si	nortcut to ConfUserAccess.exe
Target type:	Application
Target location:	enVigil
<u>T</u> arget:	Files\Pharmagraph\enVigil\ConfUserAccess.exe*
<u>S</u> tart in:	"C:\Program Files\Pharmagraph\enVigil"
Shortcut <u>k</u> ey:	None
<u>R</u> un:	Normal window
Comment:	
Eind	Target Change Icon Advanced
	OK Cancel Apply

Figure 4: Properties of Configure enVigil Users

Delete the ConfUserAccess shortcut created on the desktop. Delete all other Quick Launch\ Task Bar shortcuts to minimise confusion. The Task Bar will eventually end up similar to the following:



Figure 5: Completed Quick Launch Shortcuts (Windows XP)



Figure 6: Completed Task Bar Pinned Items (Windows 7)

Sharing the 'Logfiles' and 'Configuration' folder (server only) (Windows XP & Windows 7)

Windows XP

• Navigate to the `C:\Logfiles' and `C:\enVigilConfigs*ConfigName*' folder and right click it to access its properties.

71.8

Click the 'Sharing' tab and select 'Share this folder'

You c netwo folder.	an share this folder with other users on your rk. To enable sharing for this folder, click Share this	Group is set rante	_
O Do <u>n</u> ot sha	are this folder	1	
Share this	folder		AM.
S <u>h</u> are name:	Logfiles	Presiden to Remove	.ishera
Comment:		Full Control Character	0
User limit:	 Maximum allowed ○ Allow this number of users: 	Real	Ĭ.
To set permis: folder over the	sions for users who access this entwork, click Permissions.		
To configure : Caching.	settings for offline access, click Caching	<u>(8</u>	Cava
Windows Firew with other comp <u>View your Wind</u>	New Share Nall is configured to allow this folder to be shared puters on the network. dows Firewall settings		

• Check that the 'Share name' is 'Logfiles' and 'ConfigName' and check that the 'Permissions' are 'Read' for 'Everyone' then click 'OK':

Windows 7

Windows 7 requires an additional step to ensure that 'File and printer sharing' is switched on. To check this navigate as follows '*Control Panel'...'Network and Sharing Center'..'Change advanced sharing settings'*. Ensure that the 'Turn on file and printer sharing' option is selcted and click 'Save Changes':

Advanced sharing settings			
🌀 🕞 🕫 🔹 Network and Sharing Center 🔹 Advanced sharing settings	- 🛃	Search Control Panel	P
Change sharing options for different network profiles			-
Windows creates a separate network profile for each network you use. You	a can choose specific op	otions for each profile.	
Home or Work			
Public			
Domain (current profile)			
Network discovery			
When network discovery is on, this computer can see other netw other network computers. <u>What is network discovery?</u>	ork computers and dev	rices and is visible to	
 Turn on network discovery 			
C Turn off network discovery			
File and printer sharing			
When file and printer sharing is on, files and printers that you hav accessed by people on the network.	ve shared from this co	nputer can be	
 Turn on file and printer sharing 			
$\ensuremath{\mathbb{C}}$ Turn off file and printer sharing			

- Navigate to the `C:\Logfiles' and `C:\enVigilConfigs*ConfigName*' folder and right click it and chose `Share with'>'Specify people...'
- Select 'Everyone' from the drop down list box and click the 'Add' button.

Creating Startup Shortcuts (Windows XP & Windows 7)

You must create shortcuts for AuditComment.exe (server only) and enVigil.exe and copy them to emsuser's startup directory -

Windows XP -> 'C:\Documents and Settings\emsuser\Start Menu\Programs\Startup'

Windows 7 -> 'C:\Users\emsuser\AppData\Roaming\Microsoft\Windows\Start Menu\ Programs\Startup

Your enVigil.exe shortcut should point to the path of your main VCX file:

enVigil Client Demonstration Properties	
General Shortcut Compatibility Security	
enVigil Client Demonstration	
Target type: Application	
Target location: enVigil	
Iarget: igil.exe' "C:\enVigilConfigs\ABC\TopLevel.vcx"	
C:\Documents and Settings\emsuser\Start Menu\Programs\Startup	
<u>Starti</u> <u>File Edit View Favorites Iools H</u> elp	1
G Back - 🕥 - 🏂 🔎 Search 🎼 Folders 💷 -	
Address 🗁 C:\Documents and Settings\emsuser\Start Menu\Programs\Startup	💌 🄁 Go
File and Folder Tasks Image: Shortcut to AuditComment.exe Image: Shortcut to AuditComment.exe Shortcut to AuditComment.exe Image: Shortcut to AuditComment.exe Image: Shortcut to AuditComment.exe <td></td>	
 Publish this folder to the Web Share this folder Share this folder 	

Modifying enVigil behaviour via registry keys

There are a number of registry keys that modify the default behaviour of enVigil. Use the enVigil Registry Tool (EnVigilReg.exe) to modify these settings as required, more information can be found on each setting in the 'enVigil Registry Tool' section of the enVigil-FMS System Configuration Manual.

The 'System' tab of the enVigil Registry tool should be used to set the registry settings shown . These settings will ensure audit comment pop ups do not get hidden, AutoRun is disabled, Ctrl + Alt + Del is disabled and Windows logs in to 'EMSuser' windows account from boot up.

en

🝕 enVigil Registry Tool	×
Eile Action	
enVigil Client enVigil Server Drivers enVigil System About / Help	
HKEY_CURRENT_USER\Control Panel\Desktop	
Current key values	
ForegroundFlashCount : 0x00000003	
ForegroundLockTimeout: 0x00030d40	
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	
Current key values	
DefaultUserName : Administrator AutoAdminLogon : 0	
DefaultPassword: Key not found or unaccessable GinaDLL: Key not found or unaccessable	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Image: Disable AutoRun drives Current key value NoDriveTypeAutoRun 0x00000031	

NOTE: If using Windows 64 bit you **must** set the 'DefaultUserName', 'Default Password' and 'AutoAdminLogon' keys manually in regedit!

Eile Edit	View	Favorites	: <u>H</u> elp					
		p - 👢	Time Zones	*	Name	Type	Data	
		p - 👗	Tracing		(Default)	REG_SZ	(value not set)	
		P - 📕	UnattendSet		AutoAdminLogon	REG_SZ	1	
		-	Userinstallat		MutoLogonCount 3	REG_DWORD	0x00000000 (0)	
			WhemPerf		AutoRestartShell	REG_DWORD	0x00000001 (1)	
			Windows		Background	REG_SZ	000	
			Windows Ad		CachedLogonsC	REG SZ	10	
		1	Winsat		DebugServerCo	REG_SZ	no	
		14	WinSATAPI		DefaultPassword	REG_SZ	emsuser	
		þ - 🛴	WOW	*	RefaultUserName	REG_SZ	emsuser	
4					4			

🐔 enVigil Registry Too

HEREY LOCAL MACHIN

enVigil Serve

If you require the machine to be a dedicated enVigil Client (e.g. enVigil is the only software used on a day to day basis) you should set the 'Dedicated Client' setting on the 'enVigil Client' tab

Select Action->'Write values to registry' from the main menu to submit the changes.

	General Settings
VigilReg	×
Would you like to of HKEY_LOCAL_M Note: If setting up	write values to HKEY_CURRENT_USER instead ACHINE? a terminal services client then click 'YES'
	Yes No

File Action..

enVigil Client

behaviour of a terminal service client you should say 'Yes' to the dialog that prompts to change the registry keys of the HKEY_CURRENT_USER branch. You must ensure that the Windows account running the terminal services session is an administrator and has not yet been demoted otherwise access to write to the registry will be denied. See 'Appendix C -Terminal Service Setup Guide' for more information

When using the registry tool to change the

Ensure Inhibit Sleep is set on the 'enVigil Server' Tab

Disabling Ctrl+Alt+Del on Windows 7

It is not possible to disable Ctrl+Alt+Del in the same way with Windows 7. Instead the screen shown when Ctrl+Alt+Delete is key combination can be 'tweaked' so that no access to the operating system is given. Therefore the user cannot run 'Task Manager' (which gives the user the ability to run other programs) or even shutdown/restart the PC (Except by the On/Off button on the PC itself).

Type 'gpedit.msc' in the Windows 7 Search/Run toolbar and hit enter.

Navigate to the 'Ctrl+Alt+Del' Options' folder (Local Computer Policy...User Configuration... Administrative Templates...System...). Set all items to be 'Enabled' by double clicking the item and setting the 'Enabled' option:



Navigate to the 'Start Menu and Taskbar' Options' folder (Local Computer Policy... User Configuration... Administrative Templates.....). Set the 'Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands' to 'Enabled'. Note: This completely disables any ability to shutdown or restart the PC via the Windows 7 operating system, by any user. After this setting has been applied only the hardware on/off button on PC can be used. This setting is optional.

Collection File (.CLX) Permissions

If your enVigil configuration requires that the user can modify any collections (e.g. they can modify the collection of points used by LB2 Convert GRX facility) you must ensure that the file permissions for the .CLX file are set such that the EMSUser account has 'Write' but not 'Delete' permissions:

- Right click the CLX file and select Properties...
- Security tab... 'Add...', 'Advanced...' Find Now...'
- Select 'EMSuser' account...OK ... OK.
- Now in the properties screen click the 'Advanced button...'
- On the 'Permissions' tab ensure EMSUser is selected and click the 'Edit' button
- Ensure that the Allow permission are all set except the 'Full Control' and 'Delete' entries.... OK ... OK

NOTE: See the enVigil Collections section of this manual for more information.

Setting the ownership permissions of the enVigil install, logfile and configuration directories

Windows XP & Windows 7

• Navigate to the enVigil Install directory, the logfile directory (e.g. C:\Logfiles) and configuration directory (e.g. 'C:\enVigilConfigs*ConfigName'*)in turn, right click each folder to access its properties.

eneral Sharing	Security	Previous Version	s Customize	Э
Object name:	C:\Progra	m Files\Pharmagr	aph\enVigil	
Group or user nar	nes:			
& CREATOR O	WNER			
& SYSTEM				E
& Administrator	s (EMS-SE	ERVER1\Administr	ators)	
& Users (EMS-	SERVER1	(Users)		~
•				- F
To change permi	ssions, cli	ck Edit.		Edit
Pormissions for C				
OWNER	REATOR		Allow	Deny
Full control				
Modify				
Read & execut	е			=
List folder conte	ents			
Read				
Write				-
For special permi click Advanced.	issions or	advanced settings	A	dvanced
Learn about acce	ss control	and permissions		

• Select the 'Security' tab and click the 'Advanced' button.

• Select the 'Owner' tab, if the current owner is listed as 'emsuser' follow the remaining steps to change the owner

Permissions Audi	ing Owner	Effective Permiss	sions			
You can take or a	ssign owner	hip of this object i	f you have the req	uired permission	s or privileges.	
Object name:	C\Progra	n Files\Pharmagr	aph\enVigil			
Current owner:						
emsuser (EMS-S	ERVER1\en	suser)				
Change owner to:						
Name						
& Administrator	(EMS-SERV	ER1\Administrato	r)			
& Administrator	(EMS-SER	VER1\Administrate	ors)			
	_					
Edit						
Learn about obier	townership					
Lean about objet	a owneranity					

Owner										
You can take or	assign ow	ership of this	s object if y	ou have the	required p	ermission	s or privileg	es.		
Object name:	C:\Prog	ram Files\P	harmagrap	h∖enVigil						
Current owner:										
Administrator (B	MS-SERV	ER1\Adminis	strator)							
Change <u>o</u> wner t	o:									
Name										
& Administrate & Administrate	or (EMS-SE ors (EMS-S	RVER1\Adn ERVER1\Ad	ninistrator) ministrators	ē)						
Other <u>u</u> se	ers or group	S								
✓ Replace ow	ner on subc	ontainers an	d objects							
Learn about obj	ect owners	nip								

- From the 'Owner' tab click the 'Edit' button
- Ensure that the check box 'Replace owner on subcontainers and objects' is checked

• Click the 'Administrator'user from the 'Change owner to:' list and click the Apply button. Click OK on the three currently open permission dialog boxes.

Current owner: Administrator (EMS-SERVER1\Administrator)

Setting 'emsuser' password and demoting to limited user (XP & Windows 7)

- Open 'Control Panel .. User Accounts .. Local Users and Groups .. Users'
- Right click on 'emsuser' and click '*Set a password'*, then enter and confirm password as 'emsuser'. Note the use of all lower case
- Right click 'emsuser' again and select '*Properties .. Member Of'* and remove the Administrators group entry.

Setting PC start up behaviour in the BIOS

- During the boot sequence of the PC enter the system BIOS as instructed on the screen (usually 'F2')
- Under the 'Power Management' option (or equivalent), ensure that the 'AC recovery' behaviour (or equivalent) is set to 'Continue from previous state' (or equivalent). Note that the wording and location of this facility will vary according to BIOS type. Use the appropriate option to ensure that the PC starts up automatically if the AC power failed during normal operation. It is unusual to make the PC boot when power is applied, even if it was not on at the time of AC failure.

Beware! - Joining the System to a Domain

For computers intended to run as a part of a domain you should be aware that any configuration changes made prior to joining the computer to the domain may be reset by the domains group policy. Therefore you should always check each step of this document after the computer has been joined to the domain.

Domain User Accounts

If running the system on a domain you should request that the IT department sets up domain versions of the 'EMSUser', 'EMSSystem' and 'EMSAdmin' accounts. These accounts will replace the local user accounts created by the enVigil installer. The local accounts should therefore be deleted. The 'EMSUser' domain account can be a simple domain user account. 'EMSAdmin' and 'EMSSystem' **must** be domain accounts that have local administrative rights to the computer.

You **must** also repeat the **'Running the enVigil Server service as the 'EMSSystem' account'** section of this document but instead use the login creditals of the domain version of 'EMSSystem' :

Vigil Server Properties (I	ocal Computer)	
Log on as:		
Local System account	t	
Allow service to in	teract with desktop	
Ihis account	emssystem@asl.local	Browse
Password:	•••••	
Confirm password:	•••••	
Help me configure user a	ccount log on options.	

When the enVigil Server is set to run as a domain account the connection to the network and the health of the Primary and Secondary Domain Controllers becomes critical. If the PC is booted without the network connection in place, or if the Domain Controllers are unavailable, the enVigil Server will not run. This is due to Windows requiring a connection to the Domain Controllers to authenticate the request to run the processes as the domain user. If there is any doubt that the stability of the domain is not reliable then the enVigil Server can be left to run as the local 'EMSSystem' account.

Activity Check List -Highlight each step as it is completed

This contains some additional reminder steps not included in the main section of this document:

Step	Check
Power up PC for first time	
Set date/currency to UK/English	
Setup computer name as per FDS or SDS e.g. 'EMS-server', then enter a helpful computer description	
Record computer name used:	
Setup the local 'Administrator' password to be 'Administrator' (note the capital 'A')	
Setup internet connection method as `LAN' but leave IP/DNS details blank (skip that setup page)	
Setup Owner Name as 'emsuser' when asked for 'Your name' – this will create the initial account	
Remove unwanted applications such as OMCI and Anti-Virus and Dell Backup Manager	
Set Control Panel to Classic View	
Set screen resolution as 1280 x 1024 where possible. LCD screens should always use native resolution. Set blank screen saver	
Set the Windows theme to basic theme	
Setup Windows 7 logon screen (W7)	
Disable the Welcome Screen (XP)	
Setting the Administrator password (W7)	
Disable Windows Firewall(XP + W7) + Defender (W7)	
[OR] Create Firewall exceptions for DBXServer.exe, Launch.exe and DCOM port 135	
Disable Windows Security Centre Alerts	
Disable Windows Automatic Updates	
Set Local Security Policy to Classic Network Access	
Install enVigil application from enVigil Installation disk	
Set default password policy	
Configure the enVigil Server Service to run as 'EMSsystem'	
Check that the 'EMSadmin', 'EMSsystem' and 'EMSuser' user accounts are set to never expire	
Create Taskbar shortcuts. Delete unnecessary taskbar shortcuts	
Copy the configuration files from the Configuration CD in to PC's folder under 'enVigil'	
Copy all patches from the Configuration CD `enVigil' folder to the PC's `enVigil' folder	
Share the Logfiles and Configuration directories	
Configure the desktop's enVigil Client shortcut to point to your project's main VCX file	
Drag a shortcut to enVigil Client to EMSuser's 'Start Menu' – 'Startup' option	
Create and drag a shortcut to 'AuditComment.exe' to EMSuser's 'Start Menu' – 'Startup' option	

Modify enVigil behaviour if necessary using the enVigil Registry Tool:	
Including Ctrl + Alt + Del disable, Auto Run, Automatic Logon, Audit Comment always on top.	
Enable Dedicated Client if required.	
Enable Inhibit Sleep on Server tab.	
Tweak Ctrl+Alt+Del screen (W7)	
Set 'emsuser' password	
Setup any additional serial interface cards, if any. Remember to set RS485 ports to 'Half-Duplex, Auto-gating' where necessary	
Set AC recovery behaviour in the system BIOS	
Setup a local printer, if any	
Setup a local UPS, if any, including setting the power fail timings	
Make backup copies of the completed enVigil configuration folder and enVigil executables folder to a memory key. Remember to copy these to to a permanent backup device, along with any registry tweaks. Use enVigil Registry Tool 'FileSave' to save registrysettings so that you can get recover configurations in future	
Remove 'emsuser' ownership permissions for install, config and logfile directories	
Demote the 'emsuser' account to 'Limited User'	
Report the PC and check that enVigil Client starts in the correct target screen	

Notes: