Standalone Installation and Configuration Guide

IMPAX 6.5.1

Installing and Configuring

an IMPAX Standalone Station

AGFA

| see more | do more |

Copyright information

Trademark credits

Agfa and the Agfa rhombus are trademarks or registered trademarks of Agfa-Gevaert N.V., Belgium or its affiliates. IMPAX, Connectivity Manager, Audit Manager, WEB1000, Xero, TalkStation, Heartlab, and HeartStation are trademarks or registered trademarks of Agfa HealthCare N.V. or its affiliates. All other trademarks are held by their respective owners and are used in an editorial fashion with no intention of infringement.

Additional trademark credits

Sun, Sun Microsystems, the Sun Logo, and Solaris are trademarks or registered trademarks of Oracle America, Inc. in the United States and other countries.

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

CE
0413

Note: The IMPAX 6.5.1 software complies with the Council Directive 93/42/EEC Concerning Medical Devices, as amended by Directive 2007/47/EC.

Documentation warranty statement

Characteristics of the products described in this publication can be changed at any time without notice.

The information contained in this document is subject to change without notice. Agfa HealthCare N.V. and its affiliates make no warranties or representations, express, implied or statutory, with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Agfa HealthCare N.V. and its affiliates shall under no circumstances be liable for any damage arising from the use or inability to use any information, apparatus, method or process described in this document. Agfa HealthCare N.V. and its affiliates shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this manual.

2011 - 6 - 14

Manufacturer's responsibility

The manufacturer, installer, or importer will be responsible for the safety, reliability, and performance of the equipment only if:

- Installation, modifications, adjustments, changes, or repairs are performed by suitably qualified service personnel.
- The electrical installation of the site in which the equipment is used is according to an applicable safety standard (UL, CSA, or IEC/CDE).
- The equipment is used according to the instructions provided in the operation manuals.

External software licenses

(Topic number: 7696)

Information about third-party software licenses and copyrights can be found in *External software licenses* (refer to page 89).

Giving feedback on the documentation

(Topic number: 122201)

Thank you for taking the time to provide feedback. Your comments will be forwarded to the group responsible for this product's documentation.

To give feedback on the documentation

1. In an email subject line or body, list which product, version, and publication you are commenting on.

   For example, "IMPAX 6.4 SU01 Client Knowledge Base: Extended". (You can find this information in the footer of the publications.)
2. Describe the incorrect, unclear, or insufficient information. Or, if you found any sections especially helpful, let us know.
3. Provide topic titles and topic numbers where applicable.

   Including your personal contact details is optional.
4. Send the email to doc_feedback@agfa.com.

Sorry, we cannot respond directly to every submission and we cannot accept requests for changes in the product; instead, contact your product sales representative or the product's technical support channel.

Contents

Getting started

1

Understanding certain key concepts and system requirements helps ensure a successful installation.

Prerequisite knowledge: IMPAX installations

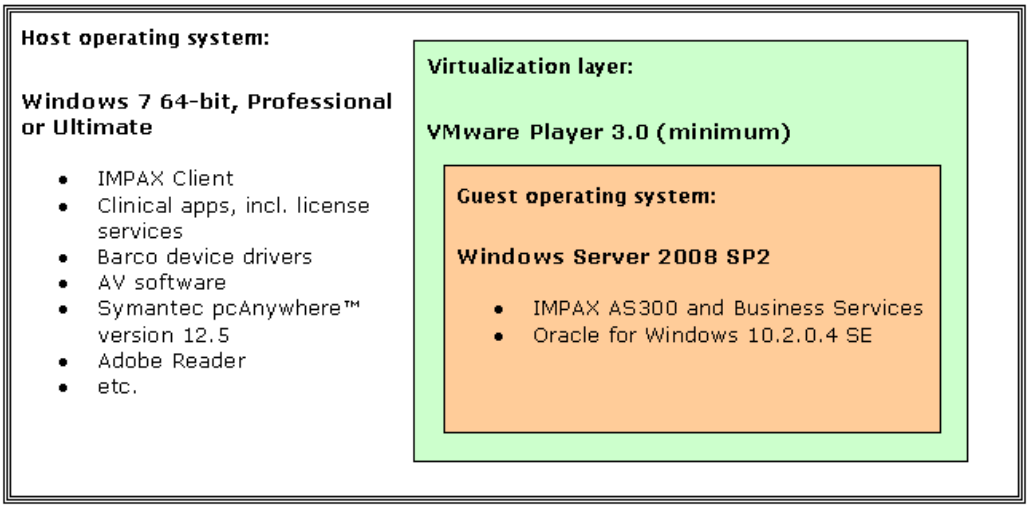
(Topic number: 7633)

The installation procedures require that you have general knowledge of computer hardware and software concepts and proficiency in operating and troubleshooting computer software.

What is an IMPAX 6.5.1 standalone?

(Topic number: 7596)

As of IMPAX 6.5, all new standalone stations are installed under Windows 7 as the host operating system. Using VMware Player, the AS300 Server and Application Server components are installed under Windows Server 2008 as the guest operating system.



Primary purpose

The primary purpose of a standalone is to provide a workstation that can operate independently of a full IMPAX cluster and can communicate (send and receive studies) with other devices via DICOM.

Situations in which standalone stations may be used include:

- Quality control workstation that sits between a modality and the main PACS cluster.
- Regular workstations in which the functionality of the new release is required prior to the main PACS cluster being upgraded. In this case, studies are typically routed to the standalone workstation from the main IMPAX cluster and reviewed there.
- Regular workstations at a small site where IMPAX is being introduced.

The IMPAX 6.5 standalone station does *not* support the following:

- Direct attached archives
- PACS Store and Remember archiving or HSM archiving
- External disk options or DAS
- Connectivity Manager and RIS integration

Recommended boundaries for optimal performance

The following are the recommended boundaries inside which a standalone station should be deployed and serviced.

Note:

Exceeding one of the boundaries may reduce performance and indicate the need for a single-server configuration instead of a standalone station; a combination of these factors—even when below the maximum value—may also indicate this need. (For more about the single-server configuration, refer to “Installing an IMPAX AS300 single-server” (topic number 67064) in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.)

- Maximum of three modalities
- Maximum of 15,000 exams/year
- Maximum of 0.5 million images/year
- Maximum yearly volume of 0.6 TB uncompressed
- Maximum of one concurrent user: Radiologist or Radiologist with QC license
- Maximum exam volume of 1.5 GB/day

Maximum peak volumes should not exceed the following:

- Exam volume peak per hour (raw data, for CR) < 1 GB/hour
- Exam image peak rate per hour (for CT) < 3000 images/hour
- Maximum of one single user

IMPAX standalone: Additional documentation

(Topic number: 7599)

The *IMPAX 6.5.1 Standalone Installation and Configuration Guide* is intended for service and administrator personnel who are installing and performing the initial configuration of an IMPAX standalone station. It provides information about the required components and instructions for the installation.

The *IMPAX 6.5.1 Standalone Upgrade Guide* is intended for service and administrator personnel who are upgrading an IMPAX standalone station. It provides information about the required components and instructions for the upgrade.

Some procedures refer you to other IMPAX guides for details; notably, these ones:

- *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*
- *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*

Details concerning customization and use of the IMPAX standalone software are provided in the *IMPAX 6.5.1 Client Knowledge Base: Extended*, *IMPAX 6.5.1 Application Server Knowledge Base*, and *IMPAX 6.5.1 Server Knowledge Base*.

All Knowledge Bases and all guides are available on the IMPAX Documentation DVD. This documentation also gets installed on the standalone station, as described in *Installing the IMPAX documentation* (refer to page 51).

What is VMware Player?

(Topic number: 108349)

VMware Player is a desktop application that lets you create, configure, and run virtual machines on a single physical machine, sharing the resources of that single computer across multiple environments. Using VMware Player, the virtual machines can:

- Share physical resources
- Run unmodified operating systems and applications
- Run the most resource-intensive applications side-by-side on the same server

The terms host and guest describe physical and virtual machines:

- Host—The physical computer on which you install the VMware Player software is called the host machine, and its operating system is called the host operating system.
- Guest—The operating system running inside a virtual machine is called a guest operating system. The virtual machine is called the guest.

For more information regarding VMware Player, see the *VMware Player Release Notes*, the *Getting Started Guide*, and the *Guest Operating System Installation Guide*, all available at the VMware Player Documentation site.

IMPAX standalone hardware and software requirements

(Topic number: 7690)

The following lists the hardware and software recommended for standalone IMPAX stations. While IMPAX standalone should work on an equivalent platform, optimal results can be guaranteed only on the recommended platform.

IMPAX standalone: Hardware requirements

(Topic number: 7689)

The following hardware is recommended for new standalone stations.

Component	Recommendation
System	**Diagnostic:** HP Z600 Workstation, HP xw6600 Workstation

Component	Recommendation
CPU	HP Z600 Workstation: Intel® Xeon® Processor E5530 (2.40 GHz, 8 MB Cache/1066 QC CPU-1) HP xw6600 Workstation: Intel® Xeon® E5410 2.33 GHz processors or better Dell Precision T5500 Workstation: Intel® Xeon® E5410 2.33 GHz processors or better
RAM	8 GB minimum
Hard drive space	Minimum: Three 450 GB or 600 GB SAS drives
RAID	HP: use RAID 1E (requires optional LSI controller for HP workstations) Dell: contact Agfa Professional Services
CD-R/DVD-R	Yes, for CD-R/DVD-R export
Network interfaces	Integrated 10/100/1000 Mbps Ethernet adapter
Video	**Diagnostic:** Barco MXRT-5200 Barco MXRT-7300 **Non-diagnostic:** NVIDIA® Quadro® FX 1700 ATI FirePro™ 3700, 3750 (third monitor board) — 256 MB RAM ATI FirePro™ 3800 — 512 MB RAM  **Note:** Windows 7 and WDDM drivers do not support BarcoMed® and older Barco MXRT boards. NVIDIA boards are not shipped with Barco boards; defaults are ATI FirePro boards. For more details, refer to Agfa's *Barco Display Platform Definition* which can be found on the Main IMPAX Knowledge Base Page in the “Additional documents” section.
Power supply	Default
Chassis	Tower
Peripherals	Scroll mouse, keyboard
Archive	Not applicable
Tape backup	Not applicable
Modem	Not applicable

IMPAX standalone: Software requirements

(Topic number: 7619)

The following software is required for new standalone stations. Unless otherwise indicated, Agfa does not provide the software as part of the installation packages.

Component	Requirement
Host operating system	Windows 7 (English) 64-bit SP1, Professional or Ultimate edition
Guest operating system	Windows Server 2008 Standard Edition SP2 (32-bit)
Remote access	Symantec pcAnywhere™ version 12.5
Database software	Oracle for Windows 10.2.0.4 Standard Edition (part of the IMPAX installation package)
Virtualization software	VMware Player 3.0 (minimum)
Other software	• Internet Explorer 7.0 or later • IIS 7.0 (integrated in operating system) • Latest version of Adobe® Reader® • AD LDS • Commonly available antivirus software • Java Runtime 1.6.0.1

Partitioning disks

(Topic number: 7032)

To store the files and programs required, create logical volumes as shown in the table in *Recommended disk partitions* (refer to page 13).

Important!

Use the logical volumes only for their prescribed functions. Do not store unnecessary files in the logical volumes; doing so may negatively affect system performance.

Recommended disk partitions

(Topic number: 120797)

When partitioning disks, consider the following:

- If you have a large disk array (RAID), create more than one CACHE logical volume. Do not allocate more than 500 GB for each logical volume.
- For Autopilot to correctly monitor cache space, each cache created in the Administration Tools must be on its own logical volume.

In either of these cases, assign drive letters to each logical volume sequentially, starting at G, and name them with the drive letter appended: CACHE-G, CACHE-H, and so forth.

You must create subdirectories in the CACHE partitions to store the imaging data. The existing SYSTEM volume on C should be used for Windows and all program files.

Note:

Throughout this document it is assumed that a CD or DVD device is assigned to drive D, and that the drive letters and names shown here are used. The volume letters and labels on your system may differ from those used here.

RAID-1E configurations

RAID 1E—also called striped mirroring, enhanced mirroring, and hybrid mirroring—is a RAID level that combines RAID 0's striping capabilities with RAID 1's mirroring protection.

Note:

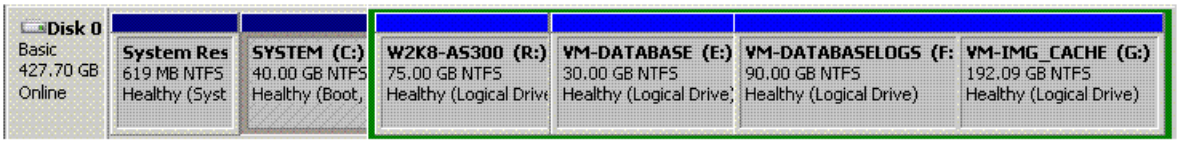
RAID 1E uses an odd number of disks to achieve its data protection goals. (RAID 10, on the other hand, requires an even number of disks.) RAID 1E has a 50% disk capacity overhead; only half of the total capacity of the array is available for use.

- Required for performance and redundancy of the operating system and database
- Limited number of disks does not allow for RAID 5
- All volumes are configured on RAID 1E
- Available capacity for 3 x 600 GB SAS disks is 900 GB (50% of raw capacity)

Disk layout examples

Windows 7 (IMPAX Client):

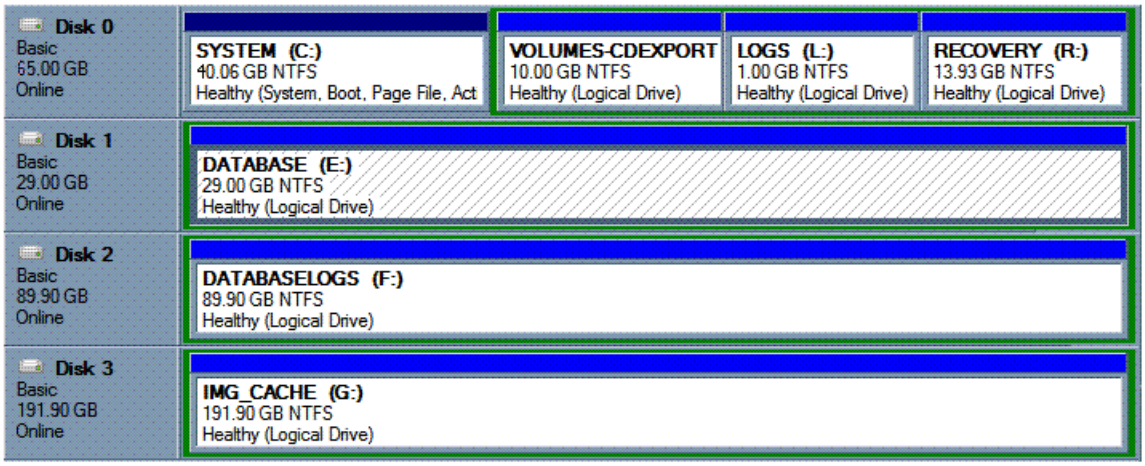
Letter	Volume label	Size	Used for
C	SYSTEM	40 GB	System files
E	VM-DATABASE	30 GB	Oracle files and database
F	VM-DATABASELOGS	90 GB	Oracle archive logs and backup.
G	VM-IMG_CACHE	Divide remaining space	IMPAX original image files
R	W2K8-AS300	75 GB	IMPAX Application Server Business Services



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
SYSTEM (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	40.00 GB	6.81 GB	17 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	619 MB	576 MB	93 %
VM-DATABASE (E:)	Simple	Basic	NTFS	Healthy (Logical Drive)	30.00 GB	933 MB	3 %
VM-DATABASELOGS (F:)	Simple	Basic	NTFS	Healthy (Logical Drive)	90.00 GB	10 MB	0 %
VM-IMG_CACHE (G:)	Simple	Basic	NTFS	Healthy (Logical Drive)	192.09 GB	98 MB	0 %
W2K8-AS300 (R:)	Simple	Basic	NTFS	Healthy (Logical Drive)	75.00 GB	55.28 GB	74 %

Windows Server 2008 (IMPAX AS300 and Business Services):

Letter	Volume label	Size	Used for
C	SYSTEM	40 GB	System files
E	DATABASE-SVCS	30 GB	Oracle files and database
F	DATABASELOGS	90 GB	Oracle archive logs and backup.
G	IMG_CACHE	Divide remaining space	IMPAX original image files
L	LOGS	1 GB	Log files
V	VOLUMES	10 GB	CD-R or DVD-R images
R	RECOVERY	10 GB of restore software (13 GB)	Recovery files



Volume	Layout	Type	File System	Status	Capacity	Free Space
DATABASE (E:)	Simple	Basic	NTFS	Healthy (Logical Drive)	29.00 GB	15.33 GB
DATABASELOGS (F:)	Simple	Basic	NTFS	Healthy (Logical Drive)	89.90 GB	89.60 GB
IMG_CACHE (G:)	Simple	Basic	NTFS	Healthy (Logical Drive)	191.90 GB	191.76 GB
LOGS (L:)	Simple	Basic	NTFS	Healthy (Logical Drive)	1.00 GB	991 MB
RECOVERY (R:)	Simple	Basic	NTFS	Healthy (Logical Drive)	13.93 GB	8.51 GB
SYSTEM (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)	40.06 GB	30.99 GB
VOLUMES-CDEXPORT (V:)	Simple	Basic	NTFS	Healthy (Logical Drive)	10.00 GB	9.92 GB

Network settings

(Topic number: 120809)

New standalone stations typically have one single onboard Gigabit Ethernet interface. The onboard Network Interface Card is used for the Windows 7/IMPAX 6.5.1 Client, as well as for the IMPAX 6.5.1 Server virtual machine.

The following IP addresses are required:

- IP address for the IMPAX 6.5.1 Client
- IP address for the IMPAX 6.5.1 Server virtual machine—the IP address for modalities to connect to

Installation preparation checklist

(Topic number: 7683)

Obtain the following information and equipment before installing the Windows operating system.

Required operating system installation information	Notes
Drive letter of the CD-ROM drive (typically D)	
Organization name	
Computer name	
Windows administrator user ID and password	
Whether the network setup is Workgroup or Domain	
Which video board is on the system	
Which languages other than English the standalone station will be used in	

Obtain the following information before installing the IMPAX software.

Required IMPAX installation information	Notes
Fully qualified domain name of the standalone station.	
Whether using integrated Windows authentication, or logging into IMPAX separately from Windows. If logging in separately, what message should appear in the Client Login screen.	
Whether accessing the Client installation program from CD or from an Installation Server.	

Required IMPAX installation information	Notes
If from an Installation Server, the server name is required.	
Whether a single or any valid IMPAX user will be logging into IMPAX on this computer. For single individuals, their Windows user ID is required.	
Whether the Orthopaedic Application software is being installed. If so, whether a dongle is installed on each workstation or on a server. If the dongle is installed on a server, the server's IP address.	
Whether Voxar is being installed (for MPR, MIP and, if licensed, 3D analysis).	

Installing and configuring the host operating system

2

New IMPAX standalone stations are installed under Windows 7 as the host operating system.

After Windows 7 is installed and initially configured, other external software applications must be installed to run a new IMPAX 6.5 standalone station.

1. Installing Microsoft Windows 7

(Topic number: 104087)

Follow these instructions to install Microsoft Windows 7 for new standalone stations.

To install Microsoft Windows 7

1. Insert the Windows 7 DVD and restart the computer.
2. When prompted, press any key.
3. Follow the installation prompts.

   Select Windows 7 Professional 64-bit (single-language support) or Windows 7 Ultimate 64-bit (multi-language support).
4. Restart the computer.
5. After the computer has restarted, complete the configuration of Windows 7.

Tip:

To view an extended context menu in Windows 7, press **Shift** + right-click; for example, press **Shift** + right-click a taskbar icon and select **Restore**.

Organization Name:	Site's name
Computer Name:	As specified on order
Administration Password:	As specified on order
Date and Time:	As appropriate for the system
Networking:	Typical
Workgroup/Domain:	Talk to the site's IS department for the appropriate setting. If intending to use integrated Windows authentication, you must use Domain.

2. Installing Windows 7 SP1

(Topic number: 130089)

If using Windows 7, we recommend installing Service Pack 1.

To install Windows 7 SP1

1. Right-click **Computer** and select **Properties**.
2. If Service Pack 1 is listed under Windows Edition, you do not have to install it.

To install Windows 7 SP1

1. Go to

   http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c3202ce6-4056-4059-8a1b-3a9b77cdfdda&displaylang=en
2. Click **Continue**.
3. Choose either the 32-bit (x86) or the 64-bit (x64) version of SP1 depending on whether you are running the 32-bit or the 64-bit version of Windows 7.

   To find out which version you are running, right-click **Computer** and select **Properties**. Under System, next to System type, you can view the operating system.
4. Click **Download**.
5. To install SP1 immediately, click **Open** or **Run**.
6. Follow the instructions on your screen.
7. On the Install Windows 7 Service Pack 1 page, click **Next**.
8. Follow the instructions on your screen.

   Your computer might restart during the installation.
9. After the installation completes, log on to your computer at the Windows logon prompt.

   You might see a notification indicating whether the update was successful.

3. Creating logical volumes

(Topic number: 15469)

Before proceeding, ensure that you have determined how to partition the disks. See *Recommended disk partitions* (refer to page 13).

Creating logical volumes improves system performance.

To create logical volumes

1. Open the Windows Administrative Tools.
2. Select **Computer Management** > **Storage** > **Disk Management**.
3. Beside Disk 0, right-click **OSDisk (C:)** and select **Shrink Volume**.

   This restricts the C: drive to the specified size and moves the rest of the available disk space to Unallocated.
4. Right-click **Unallocated** and select **New Simple Volume**.
5. Follow the New Simple Volume Wizard, using the following settings:

Screen	Select
Specify Volume Size	Simple volume size in MB, as specified in the table in *Recommended disk partitions* (refer to page 13)
Assign Drive Letter or Path	• Select **Assign the following drive letter** • Select the letter specified in the table in *Recommended disk partitions* (refer to page 13)
Format Partition	• Select **Format this volume with the following settings** • File system: **NTFS** • Allocation unit size: **Default** • Volume label: As specified in the table in *Recommended disk partitions* (refer to page 13) • Select the **Perform a quick format** checkbox.

6. To create any additional partitions, right-click the **Unallocated** space, select **New Simple Volume**, and repeat the previous step.
7. Exit Disk Management.

4. Installing device drivers

(Topic number: 97907)

Device drivers are files that provide the computer with the configurations and specifications of certain hardware devices. Without the driver file, the computer is unable to communicate with the device. Configure the appropriate drivers on the standalone.

To install device drivers

1. For each network adapter installed on the server, install the network adapter driver. Do not install the SNMP option.
2. Install the Chipset Software Installation Utility.
3. Install the video drivers.

Verifying that all device drivers were correctly installed

(Topic number: 50980)

Once all device drivers have been installed, verify that the installation was completed successfully.

To verify that all device drivers were correctly installed

1. From the **Start** menu, right-click **Computer** and select **Properties**.
2. Click **Device Manager**.
3. Check all listed drivers.
4. If any errors are indicated, reinstall that type of driver.

5. Installing video drivers

(Topic number: 7768)

If using Barco cards, you must install the current set of Barco drivers, which control the video boards. Follow the installation instructions you received with the Barco CD. For complete details, refer to the manufacturer's documentation.

Note:

If you are not using Barco cards, skip these installation instructions and continue with the next topic.

6. Configuring the Windows 7 Control Panel

(Topic number: 104095)

By default, Windows 7 uses different Control Panel categories than previous releases of Windows. To make it easier to follow the procedures in this guide, change the Control Panel to display all Control Panel items.

To configure the Windows 7 Control Panel

1. Open Control Panel.
2. From the View by list, select **Small icons** or **Large icons** (depending on user preference).

   The Control Panel window refreshes to display each available Control Panel item.

7. Configuring Windows Explorer to show all files on Windows 7

(Topic number: 104101)

We recommend that you display all available files in Windows Explorer.

To configure Windows Explorer to show all files on Windows 7

1. Open Control Panel.
2. Click **Appearance and Personalization**.
3. Select **Folder Options**.
4. Switch to the **View** tab.
5. Under Files and Folders, select **Show hidden files, folders, and drives**.
6. Clear the **Hide extensions for known file types** checkbox.
7. Click **OK**.

8. Deleting the hiberfil.sys file in Windows 7

(Topic number: 118928)

We do not recommend that hibernation be enabled on production servers. Hibernation can be disabled using Control Panel, but this still leaves behind a hidden file called hiberfil.sys, in the root folder of the drive where the operating system is installed. As this file can become very large, we recommend that it be deleted.

You can disable hibernation and delete the hiberfil.sys file in one step using a command prompt.

To delete the hiberfil.sys file in Windows 7

1. In the **Start** menu, search for **cmd**. In the search results, right-click **Command Prompt** and select **Run as administrator**.
2. If prompted, type a Windows administrator user name and password, or confirm allowing the change to take place.
3. Type

   powercfg -h off
4. Exit the command prompt.
5. Restart the server.

When the server restarts, log into Windows as an administrator-level user.

9. Creating a temporary directory

(Topic number: 104107)

Having a temporary directory on the server can be useful for storing files that you do not have to keep long-term.

To create a temporary directory

1. In Windows Explorer, select the C: drive.
2. Click **New Folder**.
3. Rename the new folder **temp**.

10. Setting the primary DNS suffix for Windows 7

(Topic number: 104242)

When referring to the IMPAX Application Server component on the Windows Server 2008 guest operating system, you should use a fully qualified domain name. The fully qualified domain name consists of a host, domain name, and top-level domain. For example, machinename.networkname.hospitalname.com. By adding a primary domain name system (DNS) suffix, this default will be used during the installation and configuration of the IMPAX software.

CAUTION!

The primary DNS suffix may have already been set automatically via DHCP, for example. This default value should not be overridden.

To set the primary DNS suffix for Windows 7

1. Right-click **Computer** and select **Properties**.
2. Under Computer name, domain, and workgroup settings, click **Change settings**.

3. Switch to the **Computer Name** tab.
4. Click **Change**.
5. In the Computer Name Change dialog, click **More**.
6. Add the primary DNS suffix.
7. Click **OK** three times.
8. When prompted, restart the computer.

When the computer restarts, log into Windows as an administrator-level user.

Under Windows 7, computers that are part of a workgroup rather than a domain must register their primary DNS suffix.

To register the primary DNS suffix

1. Open Windows Explorer.
2. Right-click **Network** and select **Properties**.
3. In the Network Sharing Center, select **Change adapter settings**.
4. Right-click the Network Connection to use and select **Properties**.
5. Click **Internet Protocol Version 4** and select **Properties**.
6. In the General Tab, select **Advanced**.
7. On the DNS tab, in the DNS suffix for this connection field, type the DNS suffix.
8. Verify that the **Register this connection's addresses in DNS** checkbox is selected.
9. Click **OK** two times, and then click **Close**.

11. Changing the desktop colors on Windows 7

(Topic number: 104113)

The default desktop colors for windows and title bars may be too bright for the lighting conditions in reading rooms, particularly on diagnostic monitors. You can change these colors as needed.

To change the desktop colors on Windows 7

1. Open Control Panel.
2. Select **Appearance and Personalization**.
3. Select **Window Color**.
4. To change the background color of windows and dialogs, from the Item list, select **Window**.

   By default, windows and dialogs are pure white. White is very bright on diagnostic monitors.
5. Click **Color 1** and select an alternative color, such as gray or off-white.
6. To change the title bar color, from the Item list, select **Active Title Bar**.

   Title bars are blue by default.

7. Click **Color 1** and select an alternative color, such as dark blue or black.
8. When done, click **OK**.

After a short delay, Windows displays the new color scheme.

12. Configuring system languages

(Topic number: 10091)

You can display the IMPAX Client interface and Knowledge Base and the Administration Tools interface in various languages:

Bulgarian	Finnish	Polish
Chinese (Simplified and Traditional)	French	Portuguese
Croatian	German	Romanian
Czech	Hungarian	Russian
Danish	Italian	Spanish
Dutch	Norwegian	Swedish
English		

The language used is based on the Windows regional settings. Some initial Windows configuration is therefore required.

Installing East Asian language filesInstall East Asian files only if entering or receiving text in Chinese (Simplified or Traditional). Windows 7 Multilingual User Interface (MUI) files require a license to be used. Contact Microsoft to obtain a license for East Asian files.

Adding all required languages and selecting a default language on Windows 7

(Topic number: 104337)

If you expect IMPAX to be accessed in more than one language on this workstation, you must add each language through the Windows Control Panel. Add no more languages than are required; each language is loaded into memory when the computer starts, potentially affecting processing speed.

Note:

If the user name contains special characters due to language settings, images cannot be calibrated. Ensure that the system locale is changed to handle any special characters for a particular language.

To add all required languages and select a default language on Windows 7

1. Open Control Panel.
2. Select **Region and Language**.

3. Switch to the **Keyboard and Languages** tab.
4. Click **Change keyboards**.
5. Switch to the **General** tab.
6. Under Default input language, select the language to use by default—the one required most often.
7. Under Installed services, click **Add**.
8. From the language list, expand the language to add.

   Note:

   It may be necessary to first download and install a language (MUI) pack via Windows Update.

9. Expand **Keyboard**.
10. From the Keyboard list, select the keyboard type for this workstation. Click **OK**.

    This option specifies the keys in the Keys list that define IMPAX Client keyboard shortcuts when this language is used. (For Dutch and the East-Asian languages, English key names are always used.)
11. To add other languages, repeat the previous three steps.
12. Click **OK**.

Selecting the region for the IMPAX Client

(Topic number: 104343)

While the IMPAX Client interface can be displayed in various languages, it should be set to one region—normally, the one that matches its geographic location. The region setting affects how numbers, dates, and currencies are displayed.

To select the region for the IMPAX Client

1. In the Region and Language dialog, switch to the **Formats** tab.
2. From the Format list, select the region to use.
3. Click **Apply**.
4. Switch to the **Administrative** tab.
5. To ensure that installation and updates work correctly, under Language for non-Unicode programs, verify that the Current language for non-Unicode programs is the same as the region selected in step 2.
6. Click **Apply**. Click **OK**.

Enabling language switching from the taskbar on Windows 7

(Topic number: 104355)

If this workstation will be used by speakers of various languages, make language switching available from the taskbar.

To enable language switching from the taskbar on Windows 7

1. Open Control Panel.
2. Select **Region and Language**.
3. Switch to the **Keyboards and Languages** tab.
4. Click **Change keyboards**.
5. Switch to the **Language Bar** tab.
6. Under Language Bar, select **Floating On Desktop**.
7. Select the **Show additional Language bar icons in the taskbar** checkbox.
8. Click **OK** twice.

   A floating Language Bar appears on the desktop.
9. To have the Language Bar appear on the taskbar instead, minimize the floating bar.

   To change the Windows language, users can click the language icon in the taskbar and select a different language.

13. Installing and configuring pcAnywhere 12.5

(Topic number: 51626)

To allow remote service of the servers, install Symantec pcAnywhere software.

Note:

Not all servers are shipped with pcAnywhere. Some servers instead use Remote Desktop Connection. Install and configure pcAnywhere only when appropriate.

Installing pcAnywhere

(Topic number: 65883)

To connect to remote devices securely for support, install pcAnywhere 12.5 following the manufacturer's instructions.

Configuring pcAnywhere

(Topic number: 48237)

After installation, you must configure pcAnywhere.

To configure pcAnywhere

1. On the Desktop, double-click **Symantec pcAnywhere**.
2. At the Please Register Symantec pcAnywhere message, click **Register Later**.
3. At the prompt, click **Finish**.
4. Under Views, click **Go to Advanced view**.
5. Under pcAnywhere Manager, click **Hosts**.
6. Under Hosts, right-click **Modem** and select **Properties**.
7. On the Connection Info tab, verify that **modem** and **TCP/IP** are selected. Click **Apply**.
8. Switch to the **Settings** tab. Under Host startup, verify that **Launch with Windows** is selected. Click **Apply**.
9. Switch to the **Callers** tab.
10. From the Authentication type list, select **pcAnywhere**.
11. Click **New Item**.
12. On the Identification tab, type the login name and password, then type the password again in the Confirm password field.
13. Switch to the **Privileges** tab. Under Caller rights, select **Superuser–caller has full access rights to host machine**. Click **OK**.
14. Click **Apply**.
15. Switch to the **Security Option** tab. Under Session options, select the **Disconnect if inactive** checkbox. Click **Apply**.
16. In the Host Properties dialog, click **OK**.
17. Under Hosts section, right-click **Modem** and select **Start Host**.
18. Minimize the pcAnywhere Waiting window and confirm that the pcAnywhere icon is displayed in the system tray.
19. Close Symantec pcAnywhere.

14. Installing Adobe Reader

(Topic number: 7679)

Note:

This installation procedure requires a direct Internet connection. If the system does not have a direct Internet connection, you can use a local Software Update Server instead. To set up a Software Update Server, contact your IT department.

The IMPAX 6.5.1 guides, quick references, and task summaries ship with the product in PDF format. To view and print the files, install the latest version of Adobe Reader.

To install Adobe Reader

1. Go to http://get.adobe.com/reader.
2. Clear the checkbox for optional software such as the Google Toolbar and McAfee Scan.
3. Click **Download now**.
4. Run the install executable.
5. In the Acrobat Reader Installation Wizard, select the appropriate options on each screen. After each selection, click **Next**.

15. Installing and configuring antivirus software

(Topic number: 10269)

Install and configure the antivirus software according to the manufacturer's instructions.

Note:

Once the IMPAX software is installed, create rules in the antivirus software to exclude IMPAX processes that are running on IMPAX Clients and Servers. For example, exclude .dcm and .inf files on IMPAX Client workstations and IMPAX web services on Application Servers.

16. Installing VMware Player 3.x

(Topic number: 108352)

Before proceeding with the VMware Player installation, ensure that you have the correct product installation locations or CDs for VMware Player, IMPAX AS300 Server software, and IMPAX Application Server software.

You can download VMware Player from http://www.vmware.com/products/player/.

To begin creating and configuring a virtual machine on the standalone station, you must install VMware Player on the Windows host. Once installed, VMware Player runs the virtual machine in a separate window.

After installing VMware Player, you can install the virtual machine components, including Windows Server 2008 (the guest operating system), Oracle Server on Windows, IMPAX Server software, and the Application Server software (IMPAX Business Services).

Manually installing VMware Player

(Topic number: 121881)

To begin creating and configuring virtual machines you must install VMware Player on the Windows host of your IMPAX Standalone station.

To manually install VMware Player

1. Download the VMware Player 3.0 installer file at https://www.vmware.com/products/player/faqs.html and save it to a directory in your system.
2. From the directory where you saved the installer file, run the VMware-player-3.0.1-227600.exe.
3. On the Welcome installation wizard screen, click **Next**.
4. On the Destination Folder screen, do not change the default location, and click **Next**.
5. On the Shortcuts screen, select each checkbox to create shortcuts in all the available places. Click **Next**.

   The Desktop icon is removed after VMware Player is configured.
6. On the Ready to Perform the Requested Operations screen, click **Continue**.
7. On the Setup Wizard Complete screen, to restart your station, click **Restart Now**.

   VMware Player is installed and ready to be configured.

Configuring VMware Player

(Topic number: 121886)

After installing VMware Player for the first time, on the IMPAX Standalone station, it needs to be configured so that you can run your Virtual Machine.

To configure VMware player

1. On the IMPAX Standalone station, double-click the VMware Player desktop icon.
2. On the License Agreement screen, accept the license agreement. Click **OK**.
3. On the Welcome to VMware Player screen, select **Create a New Virtual Machine**.
4. On the Welcome to the New Virtual Machine Wizard screen, select the **I will install the operating system later** option. Click **Next**.
5. On the Select a Guest Operating System screen, select the **Microsoft Windows** option.

6. From the version list, select **Windows Server 2008**. Click **Next**.
7. On the Name the Virtual Machine screen, type a name for the virtual machine.
8. Keep the default entry in the Location field. Click **Next**.
9. On the Specify Disk Capacity screen, in the Maximum disk size field, type **75.0** to adjust the maximum disk size. Click **Next**.

   This setting allows Altiris to later configure the C:\40GB, V:\10GB and R:\20GB disks.
10. On the Ready to Create Virtual Machine screen, click **Customize Hardware**.
11. On the Hardware dialog, select the **Network Adapter** device.
12. On the Device status pane, select the **Connect at power on** option.
13. On the Network connection pane, select the **Bridged: Connected directly to the physical network** option and the **Replicate physical network connection state** checkbox.
14. Click OK.
15. On the Ready to Create Virtual Machine screen, click **Finish**.

Virtual disks: Prerequisites

(Topic number: 121912)

To run a virtual machine, you need to configure at least one virtual hard disk for the virtual machine and install an operating system on it. You can configure a virtual machine to start from a CD, but you should still specify a virtual hard disk for the virtual machine. Many applications require that a hard disk be present in order to operate correctly

A prerequisite to creating the virtual disks is that all disk creation on the hosts system must be completed as follows:

Volume	Size	Layout	Type	File System	Status
VM-DATABASE	30GB	Simple	Basic	NTFS	Healthy (Logical Drive)
VM-DATABASELOGS	90GB	Simple	Basic	NTFS	Healthy (Logical Drive)
VM-IMG_CACHE	Remaining	Simple	Basic	NTFS	Healthy (Logical Drive)

Creating virtual disks

(Topic number: 121934)

You can use a virtual hard disk to run the virtual machine's operating system (the guest operating system) and to save data. The guest operating system treats the virtual hard disk as if it were a physical hard disk.

To create virtual disks

1. Start the VMware utility. **Start** > **Programs** > **VMware** > **VMware Player**.
2. Select the **IMPAX AS300 V6.5** virtual machine and click **Edit virtual machine settings**.
3. On the Virtual Machine Settings menu, click **Add**.
4. On the Hardware Type screen, select **Hard Disk**. Click **Next**.
5. On the Select a Disk screen, select **Create a new virtual disk**. Click **Next**.
6. On the Select a Disk Type screen, select **SCSI**. Click **Next**.
7. Ensure that the drives have been configured by the hosts system and make a note of the sizes used to build the virtual disks.

   A virtual disk is created for each of the disks with the maximum size of the disk pre-allocated for increased performance.
8. On the Specify Disk Capacity screen select the *Allocate all disk space now* checkbox and enter the total size of the disk to be created. Click **Next**.

   You can begin creating the VM-DATABASE drive into one virtual disk file.
9. On the Specify Disk File screen, direct the default file name to the appropriate drive by adding it to the beginning of the file.

   For example, for the default file name IMPAX AS300 V6.5-0.vmdk and VM-DATABASE (E:), you type E:\IMPAX AS300 V6.5-0.vmdk in the field.
10. To begin the virtual disk build, click **Finish**.

    Once the virtual disk is created, it is listed in the virtual machine setting menu. The two files are listed in the appropriate partition.
11. Repeat steps 1 to 10 for DATABASELOGS and IMG_CACHE.
12. After all virtual disks are created, click **OK**.

    The virtual machine is ready for Altiris to install the Windows 2008 OS.

Configuring VMware to add virtual disks

(Topic number: 121947)

Virtual disks are stored as files on the host computer or on a network file server. You can use a virtual hard disk to run the virtual machine's operating system (the guest operating system) and to save data. The guest operating system treats the virtual hard disk as if it were a physical hard disk. .

When the first stage completes, carry out the following manual VMware configuration to add the virtual disks to the new virtual machine.

To configure VMware to add virtual disks

1. Start the VMware utility. **Start** > **Programs** > **VMware** > **VMware Player**.
2. Select the **IMPAX AS300 V6.5** virtual machine and click **Edit virtual machine settings**.
3. On the Virtual Machine Settings menu, click **Add**.
4. On the Hardware Type screen, select **Hard Disk**. Click **Next**.

5. On the Select a Disk screen, select **Use an existing virtual disk**. Click **Next**.
6. Navigate to the virtual disk you want to add. Select **IMPAX-AS300-v6.5-0.vmdk**.

   For example, select the virtual disk created in the VM-DATABASE directory.
7. Click **Finish**.
8. If a prompt displays asking you to convert the VM partition, select **Convert**. Click **OK**.
9. Repeat steps 1 to 8 for DATABASELOGS and IMG_CACHE.
10. After all virtual disks are created, click **OK**.

    The virtual machine is ready for Altiris to install the Windows 2008 OS.

Removing the audio card and floppy drive from the vitual machine

(Topic number: 121952)

Removing the audio card from the virtual machine is a good practice to avoid distracting users, while viewing images, with possible warnings from the Admin tools. It is also a good practice to remove the floppy drive as this improves the system resource management.

To remove the audio card and floppy drive

1. Start the VMware utility. **Start** > **Programs** > **VMware** > **VMware Player**.
2. Select **IMPAX AS300 V6.5** and click **Edit virtual machine settings**.
3. Select **Floppy** and click **Remove**.
4. Select **Sound Card** and click **Remove**.
5. Click **OK**.

Installing the virtual machine components

3

After installing VMware Player and creating a virtual machine on the IMPAX 6.5.1 standalone station, certain components need to be installed on the virtual machine.

1. Installing and configuring Windows Server 2008

(Topic number: 98105)

After installing VMware Player and creating a virtual machine on the standalone station, follow these instructions to install and configure Microsoft Windows Server 2008 as the guest operating system on the virtual machine.

Installing Windows Server 2008

(Topic number: 94027)

Before installing the product software, Microsoft Windows must be installed. Before you begin the Windows installation, ensure that the proper CD drivers are installed.

Note:

When installing Windows Server 2008 in a virtual machine, first insert the Windows Server 2008 CD in the CD-ROM drive and then power on the virtual machine and follow the prompts to complete the installation. For more information, refer to the *Guest Operating System Installation Guide* which can be found at the VMware Player Documentation site.

To install Windows Server 2008

1. To boot the system, insert the Windows Server 2008 disc, choose an operating Window Boot Manager, and click **Next**.

2. On the Welcome screen, click **Install Now**.
3. From the list, choose **Windows 2008 Standard Edition** (**Full Installation**).
4. Accept the license agreement. Click **Next**.
5. Create a **C** partition as the location to install Windows.
6. Set the partition size to **40** GB. Click **Next**.
7. To set up Windows on the partition, click **Next** and follow the prompts to install Windows.
8. Select **Format the Partition using NTFS File System** and press **Enter**.

   The partition is formatted and files are copied. Depending on how big the partition is, this may take several minutes.
9. Follow the setup wizard.

After the installation is complete, the Initial Configuration Task screen is displayed.

Completing the initial configuration tasks for Windows Server 2008

(Topic number: 95233)

After installing Windows Server 2008, complete the initial configuration tasks as prompted.

To complete the initial configuration tasks for Windows Server 2008

1. If the Initial Configuration Tasks screen does not appear on-screen, it may have been disabled. Open it by running **C:\Windows\System32\Oobe.exe**.
2. Under Provide Computer Information, fill in the information as appropriate.
3. Under Update This Server, to ensure that Windows automatic updating and feedback is enabled, click **Enable automatic updating and feedback**.
4. In the Enable Windows Automatic Updating and Feedback dialog, select **Manually configure settings**.
5. Under Windows automatic updating, click **Change settings**.
6. In the Change settings dialog, set Windows to download but not install updates.
   a. Under Important Updates, select **Download updates but let me choose whether to install them**.
   b. Under Recommended Updates, clear the **Give me recommended updates the same way I receive important updates** checkbox.
   c. Click **OK**.
7. Close the Manually Configure Settings dialog.
8. Close the Enable Windows Automatic Updating and Feedback dialog.
9. In the Windows update dialog, click **Check for updates** and follow the prompts to install the updates.

Upgrading Windows Server 2008 to Windows Server 2008 SP2

(Topic number: 107471)

CAUTION!

This topic provides only basic upgrade instructions. For complete installation instructions, refer to the applicable topics in the Windows Server 2008 SP2 TechNet.

If Windows Server 2008 Service Pack 2 (SP2) was not installed by installing the latest Windows updates (to check, from the **Start** menu, right-click **Computer**, select **Properties**, and under Windows edition, check what version is installed), you can install SP2 from the SP2 CD or from the Web. The installation file is named Windows6.0-KB948465-*XXX*.exe, where *XXX* stands for the type of operating system (for example, x86).

To upgrade Windows Server 2008 to Windows Server 2008 SP2

1. Connect to the network or computer where you want to create the distribution folder.
2. In the shared folder, create a distribution folder for the service pack.
3. Copy Windows6.0-KB948465-*XXX*.exe into the distribution folder.
4. To install the service pack from a remote shared distribution folder, run **Windows6.0-KB948465-*XXX*.exe**.
5. Follow the instructions in the Setup Wizard.
6. When the installation process is complete, restart the computer.

When the computer restarts, log into Windows as an administrator-level user.

Adding roles and role services in Windows 2008

(Topic number: 104586)

When installing IMPAX on a machine running Windows 2008, configure the following roles and role services after Windows 2008 installation.

Roles:

- Active Directory Lightweight Directory Services (AD LDS)
- Web Services IIS Features

Role services:

- ASP.NET
- Windows Authentication
- IP and Domain Restrictions
- Dynamic Content Compression

- IIS 6 Management Compatibility

To add roles and role services in Windows 2008

1. Open the Windows Administrative Tools and select **Server Manager**.
2. Select **Roles** from the pane on the left.
3. Click **Add Roles**.
4. On the Before you begin page, click **Next**.
5. In the Add Roles wizard, select **Web Services (IIS)** and **Active Directory Lightweight Directory Services**.
6. On the Add Features Required for Web Server (IIS) dialog, click **Add Required Features**, then click **Next**.
7. For the following two screens, click **Next**.
8. In the Add Role Services dialog, select the **ASP.NET** checkbox.
9. In the Add Roles wizard, click **Add Required Roles Services**.
10. Select the **IP and Domain Restrictions**, **IIS 6 Management Compatibility**, **.NET Extensibility**, **Dynamic Content Compression**, and **Windows Authentication** checkboxes.
11. Click **Next** and follow the wizard.
12. To finish the installation, click **Install**.

    The installation could take several minutes.

Activating Windows Server 2008

(Topic number: 109368)

Windows Server 2008 must initially be activated.

To activate Windows Server 2008

1. If you have not already activated Windows Server 2008, open the Control Panel and select **System**.
2. Click the **Activate Windows now** link at the bottom of the screen.
3. Follow the on-screen prompts.

Changing the paging file setting

(Topic number: 106540)

To ensure that the server does not run out of virtual space, change the paging file settings.

Note:

For a standalone station in a virtual environment, the page file size values should be reduced as much as possible. The values recommended below are for physical systems.

To change the paging file setting

1. Open Control Panel and select **System**.
2. Under Tasks, click **Advanced System Settings**.
3. Under Performance, click **Settings**.
4. Switch to the **Advanced** tab.
5. Under Virtual memory, click **Change**.
6. Clear the **Automatically manage page file size for all drives** checkbox.
7. Under page file size for selected drive, click **Custom size**.
8. In the Initial size (MB) field, type a page file size.

   Set a value that is 1.5 to 2 times the size of the physical memory. For example, if the computer has 4 GB of RAM, set the Initial size to 8192.
9. In the Maximum size (MB) field, type the **same** value entered in the Initial size field.
10. Click **Set**. Click **OK**.
11. In the Performance Options and System Properties dialogs, click **OK**.
12. Restart the system.

Configuring Windows Explorer to show all files

(Topic number: 47547)

We recommend that you display all available files in Windows Explorer.

To configure Windows Explorer to show all files

1. Open Windows Explorer.
2. Select **Tools** > **Folder Options**.
3. Switch to the **View** tab.
4. Under Files and Folders, select **Show hidden files and folders**.
5. Clear the **Hide extensions for known file types** checkbox.
6. To save the changes, click **OK**.

Deleting the hiberfil.sys file in Windows 2008

(Topic number: 118485)

By default, in Windows Server 2008, the hibernation feature is disabled. (We do not recommend that hibernation be enabled on production servers.) Nevertheless, the hiberfil.sys file used by the hibernation service may exist on the server, in the root folder of the drive where the operating system is installed. As this file can become very large, we recommend that it be deleted.

To delete the hiberfil.sys file in Windows 2008

1. Open a command prompt.
2. Type

   powercfg.exe /hibernate off
3. Exit the command prompt.

Creating a temporary directory

(Topic number: 49277)

Having a temporary directory on the server can be useful for storing files that you do not have to keep long-term.

To create a temporary directory

1. In Windows Explorer, select the C: drive.
2. Under Organize, select **New Folder**.
3. Rename the new folder **temp**.

Supporting security certificate validation

(Topic number: 47577)

IMPAX uses Windows security certificates to connect the various IMPAX components.

To support security certificate validation

1. Launch Internet Explorer.
2. In Internet Explorer, select **Tools** > **Internet Options**.
3. In the Internet Options dialog, switch to the **Advanced** tab.
4. Under Security section, clear the **Check for server certificate revocation** checkbox.
5. Click **OK**.
6. Exit and restart Internet Explorer.

Enabling local access to Knowledge Bases

(Topic number: 10017)

To access the Knowledge Base from the IMPAX Documentation DVD or from a local drive, you must allow active content (including JavaScript) to run locally.

To enable local access to Knowledge Bases

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the Internet Options dialog, switch to the **Advanced** tab.
3. Under Security, select the **Allow active content from CDs to run on My Computer** and the **Allow active content to run in files on My Computer** checkboxes. Click **OK**.
4. For the changes to take effect, close and restart Internet Explorer.

You can now run the Knowledge Bases from the DVD or from a local drive.

Configuring IIS logging

(Topic number: 116031)

On Windows 2008 servers, IIS logging is enabled by default. You can disable IIS logging, or leave it enabled. If you choose to leave IIS logging enabled, change the location of the IIS log file to reduce the risk of server downtime.

Disabling IIS logging on a Windows 2008 server

(Topic number: 116039)

IIS logging is enabled by default in Windows 2008, and the default path for the log files is on the C:\ drive. Over time, the drive becomes full, which creates a serious downtime risk on the server. To prevent this, disable IIS logging.

Tip:

If you prefer to keep IIS logging active, change the location of the IIS log files (refer to page 41).

To disable IIS logging on a Windows 2008 server

1. Select **Start** > **All Programs** > **Administrative Tools** > **Server Manager**.
2. Expand **Roles** > **Web Server (IIS)**.
3. Select **Internet Information Services (IIS) Manager**.
4. Under Connections, expand **Sites**.
5. Select **Default Web Site**.

6. In the pane to the right of Connections, under Default Website Home, scroll down to the IIS section and double-click **Logging**.
7. In the Actions pane, select **Disable**.

IIS logging is disabled.

Changing the location of the IIS log files on a Windows 2008 server

(Topic number: 116046)

IIS logging is enabled by default in Windows 2008. The default path for the log files is on the C:\ drive. Over time, the drive becomes full, which creates a serious downtime risk on the server. If you prefer not to disable IIS logging (refer to page 40), you can avoid this risk by saving the log files in a different location.

To change the location of the IIS log files on a Windows 2008 server

1. Select **Start** > **Server Manager**.
2. Expand **Roles** > **Web Server (IIS)**.
3. Select **Internet Information Services (IIS) Manager.**
4. Under Connections, expand **Sites**.
5. Select **Default Web Site**.
6. In the pane to the right of Connections, scroll down to the IIS section and double-click **Logging**.
7. In the Logging pane, in the Directory field, enter the new location for the log files, or navigate to that location using **Browse**.

Log files are saved in the new location.

2. Completing other virtual machine configuration tasks

(Topic number: 121534)

After installing and configuring Windows Server 2008 as the guest operating system on the virtual machine, complete these other tasks.

Note:

For detailed instructions on staging an IMPAX 6.5.1 standalone station using VMware Player, refer to *Installing and Configuring VMware Player for IMPAX 6.5 Standalone Stations* which you can find on the Main IMPAX Knowledge Base Page in the "Additional documents" section, or contact Agfa Professional Services.

To complete other virtual machine configuration tasks

1. Install the VMware Tools.

For more information, refer to "General VMware Tools installation instructions" (Article ID 1014294) in the *VMware Knowledge Base* at http://kb.vmware.com/selfservice/microsites/microsite.do.

2. To increase the amount of RAM used by the Virtual Graphics Adapter:
   a. Open **Virtual Machine** > **Settings**.
   b. Click **Display**.
   c. Select the **Accelerate 3D graphics** checkbox.

      VMware Tools must be installed to take advantage of this option.
3. Create and maintain a master /etc/hosts file that can be loaded on both the physical and virtual machines. Keep these files updated and consistent.

   The /etc/hosts file contains the IP addresses and host names of the IMPAX station and all other network devices it communicates with. It is a directory that contains address listings and aliases for networked computers and peripherals. For more information, see "The /etc/hosts file" (topic number 9090) in the *IMPAX 6.5.1 Server Knowledge Base*.
4. Disable the screensaver on the guest virtual machine.

3. Installing Oracle Server on Windows

(Topic number: 65088)

Before installing Oracle Server, verify that the disk has been partitioned so that the E: drive is at least 30 GB and the F: drive is at least 90 GB. Then, because the installer is looking for differently sized drives, complete the following workaround so that the installation does not fail:

1. From the **Start** menu, right-click **Computer** and select **Properties**.
2. Click **Advanced system settings**.
3. Click **Environment Variables**.
4. Under System variables, click **New**.
5. In the New System Variable dialog, in both the Variable name and Variable value fields, type **AGFATEST**.

Important!

Before installing Oracle Server, disable all virus protection software.

Oracle is installed separately from the IMPAX AS300 Server software. For standalones, use the Oracle on Windows 32-bit DVD and install Oracle Standard Edition.

CAUTION!

The **installOracleInfo** file defines certain attributes used by the Oracle installation scripts. We do not recommend changing this file because if the file is corrupted, the Oracle installation

fails and the system provides no indication of the problem origin. If this file needs to be modified for any reason, use the Wordpad editor to view the file. After any changes are made, run the **dos2unix** command on the file so that it has the correct line endings.

To install Oracle Server on Windows

1. Insert the Oracle on Windows 32-bit DVD.
2. From the DVD drive, run **setup.bat**.

   Cygwin is automatically installed before the Oracle installer starts.
3. At the `Install client or server?` prompt, type **server**.
4. At the `enterprise or standard edition?` prompt, press **Enter** to install Oracle Standard Edition.
5. At the `What machine is repository host? [localhost]` prompt, press **Enter** to accept value `localhost`.
6. At the `Where is software repository?` prompt, if installing from the DVD drive on F, press **Enter**. Otherwise, type the DVD drive or the software repository directory.
7. At the `Temporary directory is c:/cygwin/tmp?` prompt, press **Enter** to accept the default location. Otherwise, type the directory to use.

   A series of messages appear as Oracle is installed and configured. If you receive the message `Problem in getting file info: No such file or directory`, you can safely ignore it.
8. After the `Oracle installation complete` message appears, restart the server.

Once the server restarts, log into Windows as an administrator-level user.

Verifying the Oracle for Windows installation

(Topic number: 65297)

After installing Oracle Server for Windows, verify that the installation was successful.

To verify the Oracle for Windows installation

1. In Windows Explorer, navigate to root C:\.
2. Open the **oracle_install.log** file in a text editor.
3. Check the log file contents to verify that the installation was successful.

If you spot the following error in the log file:

```
ERROR: Cannot add user to application access ACL.
```

you can ignore it.

If other problems are found, contact Agfa Support for assistance.

4. Obtaining Server license keys

(Topic number: 7637)

IMPAX uses software license keys that are unique to the station on which the software is installed. On a standalone station, a license key is required for the Network Gateway component. If upgrading from IMPAX 5.2, 5.3, 6.2, or 6.3, you must obtain a new license. If upgrading from IMPAX 6.4 or later, you can continue to use the same license.

Obtaining Server licenses for Windows stations

(Topic number: 10699)

To obtain new license keys, if this is required, email licensekey@agfa.com. To generate the license keys, Agfa must know the Ethernet MAC (Media Access Control) address of the server.

To obtain Server licenses for Windows stations

1. For each Windows server, open a command prompt and type **ipconfig /all**.

   The MAC address of all Ethernet cards installed on the station are listed. You can use any of these to generate the license from.

2. Copy one of the returned MAC addresses to a secure place.

   Ensure that you copy down the address exactly as it appears, including leading zeroes.

   Note:

   The MAC addresses contain only the alphanumeric characters 0-9 and A-F.

3. To obtain a license key for the server, send the MAC address information to licensekey@agfa.com, along with the type of component being installed on that server.

5. Installing IMPAX Server software

(Topic number: 7668)

On a new standalone station, install the IMPAX AS300 Server software on the virtual machine.

IMPAX AS300 installation programs

(Topic number: 7684)

IMPAX 6.5.1 AS300 includes four installation programs—two for 32-bit Windows, and two for 64-bit Windows.

On an IMPAX 6.5.1 standalone station, Oracle for 32-bit Windows and IMPAX AS300 32-bit are installed on the virtual machine.

Program	Purpose
setup.bat (Oracle for 32-bit Windows DVD)	Install the appropriate version of Oracle Server or Client for 32-bit versions of Windows
setup.bat (Oracle for 64-bit Windows DVD)	Install the appropriate version of Oracle Server for 64-bit versions of Windows. Not supported for standalone configurations.
as300-installer.exe (IMPAX AS300 installation DVD)	• Install or upgrade an AS300 Database Server on a 32-bit version of Windows, under Oracle or SQL Server • Install or upgrade an AS300 single-host server (including standalone and single-server configurations) • Install or upgrade an AS300 Network Gateway, Archive Server, or Curator
as300-installer-x64.exe (IMPAX AS300 installation DVD)	Install or upgrade an AS300 Database Server on a 64-bit version of Windows under Oracle

32-bit AS300 installer packages reference

(Topic number: 7682)

The standard (32-bit) IMPAX AS300 installer groups the packages to install under four sections: default, database, archive, and optional. The following tables explain each package.

Default

Default packages	Purpose
MVFCore	Installs the DICOM services for IMPAX and contains several core Windows services and database tables used by IMPAX.
MVFCache	Installs the DICOM SCU and autopilot services used by IMPAX and spftp services. MVFCache includes mvf_compressor, used for lossy compression, and cache_migration, used to migrate cache volumes from a flat to a hierarchical structure.
MVFNetworkGateway	Installs the SCP and APIP-SCP services used by IMPAX. Install this package only on stations that require Network Gateway functionality. Servers that support only internal transfers, not incoming DICOM communications, do not require it.
AdministrationTools	Installs the Java Administration Tools application for configuring and managing IMPAX. It also copies the Java Runtime Environment (JRE) self-extracting executable onto the system.

Default packages	Purpose
MVFocr	Installs the files necessary to enable Optical Character Recognition. This is an optional installation that works in conjunction with the MVFNetworkGateway package. Install it only if your system requires OCR. The OCR package installs default OCR templates to handle many different modality vendors. OCR training tools are not included with IMPAX.
VaultAgfa	Includes specific requirements and database extensions. Not required on 64-bit systems.

Database

Only one of the two Database Packages can be installed. Install these only on single-host servers or dedicated Database Servers. For new IMPAX standalone installations, only the Oracle Server package is supported.

Database packages	Purpose
Oracle Server Extension	Contains the files necessary to build an Oracle Server database to be used by IMPAX.
SQL Server Extension	Contains the files necessary to build a SQL Server 2008 database to be used by IMPAX. SQL Server 2000 is not supported.

Archive

Do not install archive packages on standalone stations.

Archive packages	Purpose
MVFhsm	Installs the HSM package.

Optional

Depending on the configuration of IMPAX being implemented, certain packages may not be supported.

On an IMPAX standalone station, the MVFCompressor package is installed; the MVFcdexport package is installed if CDs are to be exported from the station. Omit other optional packages.

Optional packages	Purpose
MVFCompressor	Installs the MVF Compressor package, which includes mvf_compressor_scheduler. The mvf_compressor_scheduler process is responsible for scheduling the lossy compression of images.
MVFCurator	Installs the Curator package. The Curator process compresses incoming images into Mitra wavelet format and stores them in the web cache. Studies compressed by the Curator process are served locally or over a network to display clients.

Optional packages	Purpose
MVFcdexport	Installs the CD Export server, used with the CD Export feature in the IMPAX Client. The CD Export server processes local burn jobs created by the IMPAX Client and prepares the zip files containing the data for the burn job. For instructions on using CD Export, refer to "Exporting and viewing images from CD or DVD" (topic number 8209) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.
MVFchangeaccepter	Installs a package related to the processing of change context (cc) objects. This feature is not required and we recommend that this package not be installed.
MVFpap	Installs the PAP package. A PACS Archive Provider (PAP) acts like a Service Class Provider (SCP) by receiving studies and allows sites to have their studies mirrored at another site through PACS Store and Remember archiving. This mirroring protects against data loss and enables studies at one PACS to be viewed at another.
MVForadg	Installs a set of scripts and tools for configuring and monitoring Oracle Data Guard. Data Guard is Oracle's high-availability solution. **Important!** Data Guard works **only** on servers running Oracle Enterprise Edition. Do not install it on a database server using SQL Server or Oracle Standard Edition, and do not include it on other types of servers (Archive Server, Network Gateway, Curator, standalone).

AS300 installer log files

(Topic number: 6780)

A log file containing detailed information about the system is created under C:\mvf\data\logs\SystemInfo.log.

Determining a password for the AgfaService account

(Topic number: 7705)

During the IMPAX Server software installation, you are prompted to create a password for the AgfaService account. The password must conform to the following requirements:

- Be at least eight characters long
- Not contain three or more characters from the user's account name
- Contain characters from at least three of the following five categories:
  - Uppercase (A to Z)

- Lowercase (a to z)
- Digits (0 to 9)
- Non-alphanumeric (for example, !, $, #, or %); avoid commas
- Unicode

Installing the 32-bit IMPAX 6.5.1 AS300 packages

(Topic number: 7144)

Use the IMPAX installer to install the necessary AS300 packages on the system. These packages are described in *32-bit AS300 installer packages reference* (refer to page 45).

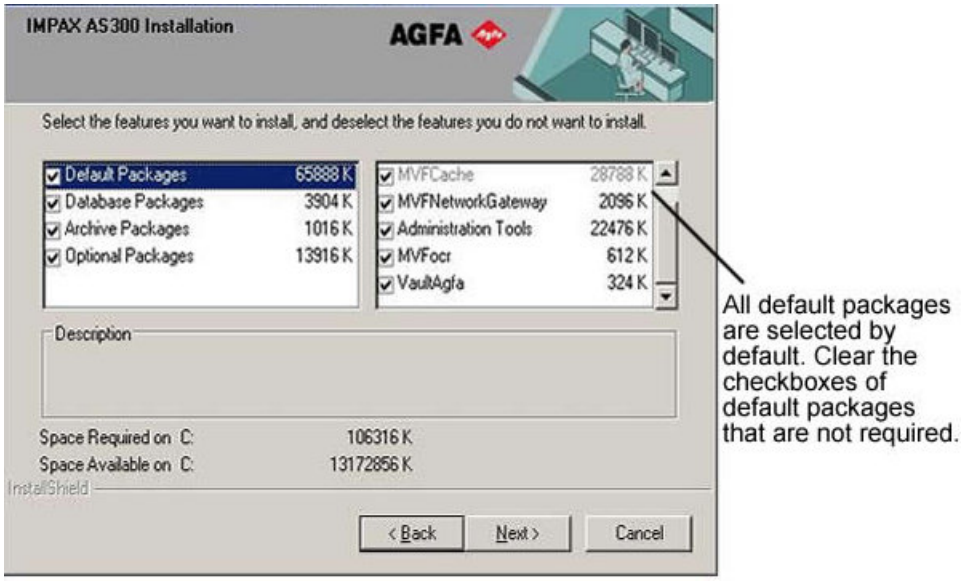
To install IMPAX AS300 Server, you must be logged into Windows as an administrator-level user.

To install the 32-bit IMPAX 6.5.1 AS300 server packages

1. Insert the IMPAX AS300 DVD.
2. Navigate to D:\programs\mvf and double-click **as300-installer.exe**.
3. Type your name (minimum three characters).

   This information is recorded in the installer log file.
4. On the Welcome screen, click **Next**.
5. On the Select features screen, all Default Packages are selected. Clear the checkboxes of any packages that should not be installed.

   Normally all Default Packages are required except, potentially, **MVFocr**.



6. Select the **Database Packages** label, then select the appropriate checkbox—normally **Oracle Server Extension**.

Oracle Server Extensions are required when using an Oracle database. Oracle is the recommended database for standard new installs.

7. Clear the **Archive Packages** checkbox.
8. Select the **Optional Packages** label, then select the checkboxes of any optional packages that should be installed.
    a. Leave the **MVFCompressor** checkbox selected.
    b. If intending to export CDs from this station, keep the **MVFcdexport** checkbox selected.
    c. Clear all other checkboxes.
9. Click **Next**.
10. In the MVF License Location dialog, browse to the location of the MVF license file and click **OK**.

    If the mvf.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.
11. When prompted, type the password for the AgfaService user.

    The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 47).
12. On the Type of Install screen, select **Create a New Database** and click **Next**.
13. On the confirmation dialog, click **Yes**.
14. On the Summary screen, to continue the installation, click **Next**.
15. To display the log file for the database scripts, when prompted, click **Yes**.
16. Check the log files for errors, then close the log files.

    The log files must be closed for the installation script to continue.
17. After all the packages have been installed, click **Yes, I want to restart my computer now**.

    If you are not prompted to restart the computer, manually restart it.

After the server restarts, log into Windows as an administrator-level user.

Confirming that the correct IMPAX AS300 packages are installed

(Topic number: 105679)

Using Control Panel, you can confirm that the correct packages are installed, and change them if necessary.

To confirm that the correct IMPAX AS300 packages are installed

1. Open Control Panel.
2. Select **Programs and Features**.
3. Select **AGFA IMPAX AS300** and click **Change**.
4. After the installer launches, click **Modify**.

5. Click **Next**.
6. Verify that the list of installed packages is correct and remove any if necessary.

   If necessary, uninstall IMPAX 6.5.1 Server (refer to page 87) and reinstall.

6. Upgrading the Internet Explorer version

(Topic number: 131184)

If running an earlier version of Internet Explorer, we recommend that you upgrade the version. To verify which version of Internet Explorer is being used, start Internet Explorer and select **Help** > **About Internet Explorer**.

To upgrade the Internet Explorer version

1. Launch Internet Explorer on a computer connected to the Internet.
2. Go to

   http://windows.microsoft.com/en-US/internet-explorer/help
3. Select the support version you want to upgrade to.
4. From this page, you can either download Internet Explorer or order it on CD.
5. Once you have obtained the software, run it on each server that needs upgrading.
6. To install the software, follow the on-screen prompts.

7. Installing Adobe Reader

(Topic number: 7679)

Note:

This installation procedure requires a direct Internet connection. If the system does not have a direct Internet connection, you can use a local Software Update Server instead. To set up a Software Update Server, contact your IT department.

The IMPAX 6.5.1 guides, quick references, and task summaries ship with the product in PDF format. To view and print the files, install the latest version of Adobe Reader.

To install Adobe Reader

1. Go to http://get.adobe.com/reader.
2. Clear the checkbox for optional software such as the Google Toolbar and McAfee Scan.
3. Click **Download now**.
4. Run the install executable.

5. In the Acrobat Reader Installation Wizard, select the appropriate options on each screen. After each selection, click **Next**.

8. Installing and initially configuring IMPAX Business Services

(Topic number: 120812)

When installing a new standalone station, after the IMPAX Server software is installed, install and configure the IMPAX Business Services and related software on the virtual machine.

Installing the IMPAX documentation

(Topic number: 15523)

IMPAX is shipped with three sets of documentation: the *IMPAX 6.5.1 Client Knowledge Base: Extended* and related guides, the *IMPAX 6.5.1 Application Server Knowledge Base* and related guides, and the *IMPAX 6.5.1 Server Knowledge Base* and related guides. The IMPAX documentation set appears on its own installation DVD.

To install the IMPAX documentation

1. Insert the IMPAX Documentation DVD.
2. From the DVD root, double-click **IMPAXDocumentationSetup.exe**.

   A `Preparing to install` message appears.
3. On the Welcome screen, click **Next**.
4. On the Setup Type screen, select the appropriate option and click **Next**.
   - To install all documentation in all available languages (up to 24 languages), select **All Documentation**.
   - To install all English-language documentation, select **All English Documentation**. This is the default.
   - To select which documentation to install in which languages, select **Select Documentation to Install**.
5. If you selected Select Documentation to Install, on the Choose Features screen, you can select particular Knowledge Bases or languages to install.
   - To install the IMPAX Client Knowledge Base in two or more languages, click  beside the name of the language to install and select **This feature will be installed on the local hard drive**. (Note that English must be installed.)
   - To **not** install the IMPAX Server, IMPAX Application Server, or IMPAX Client documentation, click  beside the appropriate label and select **This feature will not be available**.

6. On the Ready to Install the Program screen, click **Install**.

   Installation progress messages are displayed.

7. On the InstallShield Wizard Completed screen, click **Finish**.

The selected IMPAX documentation is now installed. Shortcuts appear in the Start menu and on the desktop. For additional details on viewing the translated documentation on the IMPAX Client see Viewing translated documentation from the IMPAX Client Help menu

Installing the IMPAX Business Services

(Topic number: 9873)

The IMPAX Business Services must be installed.

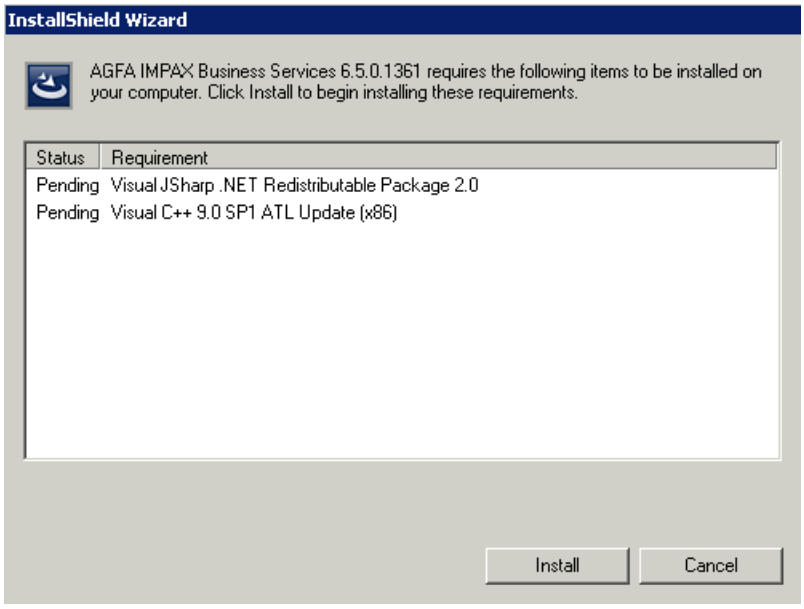
To install the IMPAX Business Services

1. Insert the IMPAX Business Services CD.
2. Navigate to the appserver folder, which contains the Business Services software.
3. Run **AGFA IMPAX Business Services Setup.exe**.
4. Select the required software packages to install.

   The following packages must be installed prior to the Business Services installation.

   - Visual JSharp .NET 2.0
   - .NET Framework 3.5 SP1
   - Visual C++ 9.0 SP1 ATL Update (x86)

   If any of these packages are listed in the InstallShield Wizard dialog, select them. If any of these packages do not appear in the list, those packages are already installed.



5. Click **Install**.
6. On the Welcome screen, click **Next**.
7. At the license agreement, select the **I accept the terms in the license agreement** checkbox. Click **Next**.
8. On the Web Services Installation Folder screen, click **Change**.
9. Select **E:\wwwroot** as the location for the Web Services. Click **OK**.

   Changing the location of the Web Services installs all of the web services to the same directory.
10. Click **Next**.
11. On the Setup Type screen, click **Custom**. Click **Next**.
12. On the RIS screen, click **Next**.
13. Click **Install**.

    The IMPAX Business Services are installed.
14. When complete, optionally select the **Show the readme file** and **Launch IMPAX Business Services Configuration tool** checkboxes.
15. Click **Finish**.

The IMPAX Business Services are installed. If selected, the Configuration Tools are displayed.

Configuring IIS error messages on Windows Server 2008

(Topic number: 109425)

You must configure IIS to display the correct error message if the Knowledge Base cannot be found.

To configure IIS error messages on Windows Server 2008

1. Open the Windows Administrative Tools and select **Internet Information Services (IIS) Manager**.
2. Expand ***computer_name*** > **Sites** > **Default Web Site**.
3. In the Features view, scroll down to the IIS category and double-click **Error Pages**.
4. From the list, double-click the **404** row.
5. In the Edit Custom Error Page dialog, select **Execute a URL on this site**.
6. In the URL field, type **/AgfaHC.LanguageRedirect/LanguageRedirect.aspx**.
7. Click **OK** to close the dialog.
8. To close the Internet Information Services (IIS) Manager window, select **File** > **Exit**.

Verifying the Business Services installation

(Topic number: 7598)

You can verify the IMPAX Business Services installation by checking whether IIS works.

To verify the Business Services installation

1. Open a web browser and connect to **http://localhost**.
2. Verify that the "IMPAX Documentation" page is displayed.

   or

   If the IMPAX Documentation has not been installed on the server, that the "Welcome to IMPAX 6.5.1" page is displayed.

Establishing an SSL connection

(Topic number: 11279)

Use the Security Wizard to generate a certificate request to submit to a trusted certificate authority, import an SSL certificate, and assign it to services.

Creating an SSL certificate request

(Topic number: 7709)

Generate a certificate request that can be submitted to a trusted certificate authority (refer to page 55). The information required by the wizard to create the certificate request is prefilled from the network settings of the server. If you already have the SSL certificate from the certificate authority, skip this topic and go to *Importing an SSL certificate in the Security Wizard* (refer to page 56).

To create an SSL certificate request

1. To open the Security Wizard, select **Programs** > **Agfa HealthCare** > **Business Services** > **Security Wizard**.
2. On the Select a method screen, select **Work with SSL certificates**. Click **Next**.
3. On the Agfa Certificate screen, select **Create a new certificate request**. Click **Next**.
4. On the Organizational information screen, type the name of your Organization and Organizational Unit. Click **Next**.
5. On the Your site's common name screen, type the fully qualified domain name of the machine or load balancer, as appropriate, if it is not present by default. Click **Next**.

   The fully qualified domain name consists of a host, domain name, and top-level domain. For example, machinename.networkname.hospitalname.com. You should be able to ping the fully qualified domain name.
6. On the Geographical Information screen, type the Country/Region, State/Province, and City/Locality information for your site. Click **Next**.

   You must type a two-letter code (ISO standard) in the Country/Region and State/Province fields, or the SSL certificate request will fail.

   Example:

   For Country/Region: United States, type **US**.

   For Province/State: North Carolina, type **NC**.

7. On the Certificate Key Length screen, select the length of the certificate key from the list. Click **Next**.
8. On the Certificate Request File Name screen, in the File Name field, browse for or type a location and name for the request file.

   The default file name and location is C:\certreq.txt. To avoid overwriting certificate request files, ensure that each request file has a unique name.
9. To copy the information in the certificate file to the Clipboard, select the **Copy certificate file contents to clipboard on creation** checkbox.

   By selecting this option, the information in the certificate request is copied to the Clipboard so that you can paste it into the certificate authority's online application form.
10. If your system uses a load balancer, select the **Allow certificate to be installed on multiple machines (exportable)** checkbox. Click **Next**.
11. On the Request File Summary screen, click **Finish**.

    The certificate request is created and saved as a .txt file.
12. In the Certificate Enrollment dialog, click **OK**.

Submitting a certificate request to a certificate authority

(Topic number: 11411)

You cannot use the Application Server component without an SSL certificate. Purchase a 128-bit encrypted SSL certificate from a trusted Certificate Authority to guarantee security.

To submit a certificate request to a certificate authority

1. Create an SSL certificate request (refer to page 54).
2. Open a web browser and go to the website of a certificate authority.

   For a list of trusted certificate authorities, consult *Viewing the list of certificate authorities in Internet Explorer* (refer to page 55).
3. Purchase a **128-bit encrypted SSL certificate** by following the instructions on the certificate authority's website.

   The exact steps may vary, depending on which trusted certificate authority is used.

After you have received the SSL certificate from the certificate authority, import and assign it.

Viewing the list of certificate authorities in Internet Explorer

(Topic number: 50237)

Use a trusted certificate authority when requesting an SSL certificate.

To view the list of certificate authorities in Internet Explorer

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options**.

3. Switch to the **Content** tab.
4. Under Certificates, click **Certificates**.
5. Switch to the **Trusted Root Certification Authorities** tab.

   The list of certificate authorities recognized by Internet Explorer is displayed.

Tip:

Trusted certificate authorities include Verisign http://www.verisign.com, Thawte http://www.thawte.com, Entrust http://www.entrust.com, Comodo http://www.comodogroup.com, and Globalsign http://www.globalsign.com. These certificate authorities are already trusted by Internet Explorer.

If using your own certificate authority, on each Client, ensure that Internet Explorer is configured as follows: the **Check for publisher's certificate revocation** option is selected and the **Check for server certificate revocation** option is cleared.

Importing an SSL certificate in the Security Wizard

(Topic number: 11422)

Once you have received an SSL certificate from the certificate authority, you must import it through the Security Wizard before assigning it. When installing an SSL certificate, assign it to all available services.

To import an SSL certificate in the Security Wizard

1. Open the Security Wizard.
2. On the Select a method screen, select **Work with SSL certificates**. Click **Next**.
3. On the Agfa Certificate screen, select **Import a certificate from file**. Click **Next**.
4. On the Certificate Import information screen, click **Browse** and navigate to the certificate file.

   Certificate files have a .cer extension.
5. Click **Finish**.

The certificate is now imported and must be assigned to services.

Assigning an SSL certificate in the Security Wizard

(Topic number: 50234)

Once you have received and imported an SSL certificate from the certificate authority, assign it to all available services.

To assign an SSL certificate in the Security Wizard

1. Open the Security Wizard.
2. On the Select a method screen, select **Work with SSL certificates**. Click **Next**.

3. On the Agfa Certificate screen, select **Assign an existing certificate to services**. Click **Next**.
4. On the Available Certificates screen, verify that the imported certificate is selected. Click **Next**.
5. On the Available Services screen, select all services listed, including **Internet Information Systems** and **ADAM/AD LDS: Agfa Healthcare**. Click **Finish**.
6. At the `Successfully applied certificate to services` prompt, click **OK**.

The certificate is now installed and will be used by all selected services.

Creating the administration account

(Topic number: 7708)

The administration account must be created for logging into the IMPAX Client and configuring additional users.

Note:

The administration account is available only after an SSL certificate has been installed on the standalone station.

To create the administration account

1. Open the Security Wizard.
2. On the Agfa Security Wizard screen, select **Work with the Application Server default settings**. Click **Next**.
3. On the Web Services URL Configuration screen, click **Next**.
4. If you are using a production license, set up an administrator user.
   a. On the User Management screen, select **Add Administrator**.
   b. Type the user name and password
   c. To confirm the password, type it a second time.
   d. Click **Next**.
5. Click **Add Administration License**.
6. Browse to the location of the license.

   The default location for licenses is C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool. The site received an administrator license with the IMPAX 6.5.1 installation package.
7. Select the administration license and click **Open**.
8. Click **Finish**.
9. At the prompt, click **OK**.

   The administration license is installed and activated.

The administration account has been created and the administrator user can log into the IMPAX Client (once it is installed).

Connecting to the AD LDS server

(Topic number: 106279)

The AD LDS server is a database that maintains all the security around user profiles, access controls, and station information on systems running Windows Server 2008. Connect to the AD LDS server so IMPAX Client users can be added.

To connect to the AD LDS server

1. Open the Business Services Configuration Tool.
2. Switch to the **Security** tab.
3. In the Server Fully Qualified Hostname field, type the domain and host name of the AD LDS server.

   The fully qualified domain name consists of a host, domain name, and top-level domain. For example, machinename.networkname.hospitalname.com.

   Tip:

   When the primary instance of AD LDS is on the server you are configuring, the fully qualified domain name and port number are automatically populated from the DSN information on the computer.

4. Type the Port number of the AD LDS server.

   The default port number of the AD LDS server is 636.
5. Click **Apply**.

Creating an Oracle ODBC data source

(Topic number: 59290)

When using an Oracle database, configure the Application Server component communication with that database.

To create an Oracle ODBC data source

1. Open the Windows Administrative Tools.
2. Double-click **Data Sources (ODBC)**.
3. Switch to the **System DSN** tab.
4. Click **Add**.
5. In the Create New Data Source dialog, select **Oracle in ohome**.
6. Click **Finish**.

7. As the Data Source Name, type **mvf_ora**.
8. Type a description, if needed.
9. As the TNS Service Name, type

   MVF.world
10. As the User ID, type

    mvf

    The user ID must be lowercase.
11. Click **Test Connection**.
12. In the Oracle ODBC Driver Connect dialog, type the Service Name **MVF.world**, User Name **mvf**, and Password **mvf**.
13. Click **OK**.
14. The message `Connection to Oracle database successful` appears. Click **OK**.

    If the test fails, verify that the information is correct and test the connection again.
15. To save the changes and close the dialog, click **OK**.
16. To save the new source and exit the ODBC Data Source Administrator dialog, click **OK**.

    The Oracle ODBC data source has been created.
17. Repeat steps 7—16. In step 7, as the Data Source Name, type

    mvf

Connecting the Business Services to an Oracle database

(Topic number: 11355)

Configure the Business Services to communicate with the Oracle database that contains all the patient information.

To connect the Business Services to an Oracle database

1. Open the IMPAX Business Services Configuration Tool.
2. Switch to the **Database** tab.
3. Under PACS Database Settings, select **Oracle**.
4. As the Oracle Service Name, type **MVF.WORLD**.
5. In the Business Services Configuration Tool, click **Test**.
6. If the message `Connection to Oracle database successful` appears, click **OK**.

   If the test fails, verify that the Oracle Server Name is correct and test the connection again.

Extending the database schema

(Topic number: 7680)

The Extend Schema function adds additional tables required by the IMPAX Client. This process is completed during the initial configuration of the Application Server and is required only once. If you try to extend the database a second time, the function notifies you that the database has already been extended and stops.

To extend the database schema

1. If not already running, open the Business Services Configuration Tool.
2. Switch to the **Database** tab.
3. Ensure that your SQL or Oracle (refer to page 59) database connection is configured.
4. Click **Extend Schema**.
5. In the confirmation dialog, click **Yes**.

   Note:

   If you receive the error message `osql is not recognized as an internal or external command, connection failed`, restart the Business Services Configuration Tool and repeat all previous steps.

6. Click **OK**.

   The database schema is extended. This process takes only a few seconds to complete.
7. In the command prompt dialog, when prompted, press any key.
8. Verify that no errors appear in the log file, and close the dialog.
9. In the Success dialog, click **OK**.

Armoring the Application Server

(Topic number: 7741)

After completing the previous Application Server configuration steps, you must apply them. When you apply these settings, the security settings for the Application Server are also applied.

To armor the Application Server

1. On any tab of the IMPAX Business Services Configuration tool, click **Apply**.
2. If a *Please enter an IP Address for Connectivity Manger [sic] IP Filtering* message appears, click **OK**.
3. Switch to the **Web Services** tab.
4. Under the Connectivity Manager IP Filtering section, in the Grant Access to IP textbox, type **127.0.0.1** as the IP address.

5. Click **Add**.
6. After the IP has been added, to apply the change, click **Apply**.

   All configuration changes and the armoring settings are applied to the Application Server components. This process may take a few minutes to complete.
7. If prompted for an Enterprise URL Hostname, type the fully qualified host name of this standalone station.
8. Click **OK**.
9. In the Agfa Configuration Results dialog, click **OK**.

Important!

When configuring the Application Server on Windows 2003 SP2, including IMPAX RIS, the Configuration Results screen and the log file (c:\impax\logs\configurator.log) display an Oracle error that should be ignored. Example: `ERROR UpdateDatabase(): Unable to save report source configuration to the database. Any changes made to report sources will be lost.` This error does not display on Windows 2008 SP2 server.

9. Synchronizing clocks on Windows-based IMPAX systems

(Topic number: 6752)

If the system time on the Application Server and the image server (ASPFTP server) differs, the authentication tickets provided by the IMPAX Client are rejected by the ASPFTP server and image retrieval fails. You must configure the IMPAX systems to automatically synchronize their system time with a common server and remain synchronized.

Note:

Also ensure that the time zone for the computer is set correctly.

The instructions that follow use the synchronization feature built into the operating system. When configured, Windows Time Service sets and synchronizes the system time with a standard time server.

Synchronizing Windows servers to an external time source

(Topic number: 58717)

Synchronize the Windows Server 2003 and Windows Server 2008 servers on your network to an external time source to ensure that image data streaming operates correctly.

CAUTION!

Serious problems might occur if you modify the registry incorrectly. These problems might require that you reinstall your operating system and there is no guarantee that these problems can be solved. We recommend that you back up the registry before you change it, so that you can back out the changes if necessary.

To synchronize Windows servers to an external time source

1. To open Registry Editor, select **Start** > **Run**, type **regedit**, and click **OK**.
2. To change the synchronization server to NTP, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type** subkey, change the REG_SZ value from NT5DS to **NTP**.
3. To specify if the local machine is a local time server, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags** subkey, change the REG_DWORD value to **5**.
4. To enable the NTPServer, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled** subkey, change the REG_DWORD value to **1**.
5. To specify where the computer obtains time stamps, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer** subkey, enter the list of DNS names or IP addresses.

   If you use DNS names, append **,0x1** to the end of each DNS name.
6. To set the poll interval, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval** subkey, change the REG_DWORD value to the number of seconds between each poll.

   The recommended value is **900** Base **Decimal**, which polls the time server every 15 minutes.
7. To specify the maximum positive difference that triggers a synchronization, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection** subkey, change the REG_DWORD value to the maximum number of seconds.

   The recommended value is **3600** Base **Decimal**.
8. Similarly, to specify the maximum negative difference that triggers a synchronization, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection** subkey, change the REG_DWORD value to the maximum number of seconds.
9. Exit the Registry Editor.
10. To stop and restart the Windows Time server, at a command prompt, type **net stop w32time && net start w32time**.

    It may take up to an hour for this to take effect.

For more information, refer to the Microsoft Knowledge Base article KB 816042.

Synchronizing Windows servers to an internal time source

(Topic number: 58720)

Synchronize the Windows Server 2003 and Windows Server 2008 servers on your network to ensure that image data streaming operates correctly. To configure the Primary Domain Controller (PDC) master without using an external time source, change the announce flag on the PDC master. Choose either the Application Server or the AS300 server as the PDC master and synch the other servers to it.

CAUTION!

Serious problems might occur if you modify the registry incorrectly. These problems might require that you reinstall your operating system and there is no guarantee that these problems can be solved. We recommend that you back up the registry before you change it, so that you can back out the changes if necessary.

To synchronize Windows servers to an internal time source

1. To open Registry Editor, select **Start** > **Run**, type **regedit**, and click **OK**.
2. To specify if the local machine is a local time server, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags** subkey, change **REG_DWORD** to **A**.
3. Exit the Registry Editor.
4. To stop and restart the Windows Time server, at a command prompt, type **net stop w32time && net start w32time**.

   It may take some time for this to take effect.

Note:

The PDC master must not be configured to synchronize with itself.

Synchronizing with a time server when the IMPAX computer is not a member of a domain

(Topic number: 58572)

To ensure that image data streaming operates correctly when the IMPAX computer is not a member of a domain, use the synchronization feature built into the operating system.

To synchronize with a time server when the IMPAX computer is not a member of a domain

1. Open Control Panel.
2. Select **Date and Time**.
3. Switch to the **Server Internet Time** tab.

4. In the list, type or select the time server to synchronize with.

Synchronizing with a time server when the IMPAX computer is a member of a domain

(Topic number: 58569)

To ensure that image data streaming operates correctly when the IMPAX computer is a member of a domain, use the synchronization feature built into the operating system.

To synchronize with a time server when the IMPAX computer is a member of a domain

1. Open a command prompt.
2. Type

   w32tm /config /syncfromflags:manual /manualpeerlist:*time_server*

   where *time_server* is the DSN name or IP address of the time server. The *time_server* can be any Windows- or Solaris-based server.
3. To update Windows Time Service to use the new configuration, type

   w32tm /config /update
4. To synchronize the clock, type

   w32tm /resync

10. Configuring the IMPAX Server components

(Topic number: 7720)

Once the Application Server software is installed and configured on a new standalone station, you can do the initial IMPAX 6.5.1 Server and the final Business Services configuration steps.

Configuring Data Execution Prevention (DEP)

(Topic number: 7192)

Data Execution Prevention (DEP) is on by default for all Windows programs. DEP is designed to help prevent damage from viruses and other security threats by marking some memory locations "non-executable" so that malicious code cannot be executed from memory locations that only Windows and other programs should use. This increased security, however, can cause problems with some programs that require this memory space, including IMPAX. If DEP remains on, you may encounter problems with Curator, ddo_store, or CD burns, among other features.

Note:

To successfully configure DEP, the directory C:\mvf\bin must already exist. Also, not every executable listed in step 7 may appear in the directory.

To configure Data Execution Prevention (DEP)

1. Right-click **Computer** and select **Properties**.
2. Under Tasks in the left pane, select **Advanced system settings**.
3. If not selected, switch to the **Advanced** tab.
4. Under Performance, click **Settings**.
5. Switch to the **Data Execution Prevention** tab.
6. In the Performance Options dialog, select **Turn on DEP for all programs and services except those I select**.
7. For each IMPAX executable in the list that follows, click **Add**, navigate to C:\mvf\bin, select the executable, and click **Open**:
   a. **ddo_create.exe**
   b. **ddo_store.exe**
   c. **mvf_scp.exe**
   d. **mvf_scu.exe**
   e. **mvf_compressor.exe**
   f. **mvf_autopilot.exe**
8. Click **OK** and close all open dialogs.
9. Restart the system.

When the server restarts, log into Windows as an administrator-level user.

Performing a warm backup of the Oracle database

(Topic number: 66644)

With a warm backup, the database does not have to be shut down. Warm backups are therefore less disruptive than cold backups, in which the database does have to be shut down.

To perform a warm backup of the Oracle database

1. Log into the standalone station as the **AgfaService** user.
2. In a command prompt, change to the **C:\mvf\bin** directory.

   In a command prompt, change to the **C:\Connectivity-Oracle\mcf\etc** directory.
3. In the command prompt, type **bash runbackup**.

   The backup may take a significant amount of time.

Logging into the IMPAX Administration Tools

(Topic number: 8213)

Many IMPAX Server configuration tasks must be performed in the IMPAX Administration Tools. This topic explains how to log into the Administration Tools. A valid user ID and password are required.

Note:

Passwords are case-sensitive; *PASSWORD* is not the same as *password*.

To log into the IMPAX Administration Tools

1. On the server, select **Start** > **All Programs** > **IMPAX Administration Tools** > **Administration Tools**.
2. Select the Domain to connect to.
3. Type the user ID and password.
4. Press **Enter** or click **Login**.

Tip:

After you log in under your user ID for the first time, your user ID may appear as a button on the login screen. (This can be configured by the system administrator.) If your user ID appears as a button, you can click your User ID and type your password to log in.

Creating cache volumes

(Topic number: 9114)

Use the Cache Manager to specify partitions or subdirectories on stations to use as image cache or web cache. You can create cache volumes only from the server where the Administration Tools are installed; you cannot do so remotely through a browser login.

To create cache volumes

1. On the Daily tab, click **Cache Manager**.
2. Click **New Cache Volume**.
3. In the Add Volume dialog, select the Volume Type to create: **Image Cache**.
4. From the Station list, select the station to set up the cache on.
5. In the Path field, type the path for the new cache volume.

   You must specify the cache locations using UNC paths.
6. Click **Add**.

7. In the Warning dialog, verify that the path is correct and click **Yes**.
8. To select the cache volume to fill with images first, select the volume in the list and click **Increase Priority**  or **Decrease Priority**. 
9. If the cache volume is hosted remotely or if you are setting up network area storage (NAS), after the cache is created, create a user account for the ImpaxServerUser on the system hosting the cache and give the ImpaxServerUser full read, write, and execute permissions on the cache folder.

Considerations when defining the cache volume path

When creating a cache on a Windows system, do not use a trailing slash or backslash at the end of the volume path. For example, when creating an image cache, do not type \\server\f$\CACHE1\; instead, use \\server\f$\CACHE1. Defining the cache volume with a trailing slash or backslash can cause problems in retrieving images from the cache.

Note:

If cache volumes are assigned to a subdirectory on a partitioned hard drive, the values shown in the Available and Occupied columns in Cache Manager refer to the entire partition, not the subdirectory.

Logging out of the IMPAX Administration Tools

(Topic number: 8212)

Log out of the Administration Tools when you leave the station for any length of time. Logging out protects patient confidentiality and maintains system security.

To log out of the IMPAX Administration Tools

1. In the top-right corner of the Administration Tools, click **Exit**. 
2. To close the Administration Tools window, click **Exit**. 

When you log out, IMPAX continues to function in the background.

Setting the logging levels

(Topic number: 7623)

Set the log level for each web service, Windows service, and application to capture the appropriate amount of information about its behavior.

To set the logging levels

1. Open the Business Services Configuration Tool.
2. Switch to the **Logging** tab.

3. Switch to the **Web Services** tab.
4. Locate the web service in the list.
5. From the Log Level list, select the appropriate logging level.

   Note:

   The Debug log level can cost about 10% or more extra time in performance. Generally, use it only temporarily, when troubleshooting a specific issue.

   The log level is set for the web service.
6. Repeat these steps for each item on the Web services, Windows service, and Application tabs.

Performing other IMPAX Business Services configurations

(Topic number: 9879)

If the station requires other configurations, such as customizing the Login message, supporting East Asian characters in Study Comments, using Windows authentication, or configuring RIS connections, refer to the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide* or the *IMPAX 6.5.1 Application Server Knowledge Base* for details.

Running Healthcheck from a URL to check the status of web services

(Topic number: 11405)

Healthcheck checks the status of each web service running on the Application Server. When you run Healthcheck, it attempts to connect to each of the web services. If it succeeds, Healthcheck sets the status to Passed (green) . If Healthcheck fails, the status is set to Failed (red) . The comment field indicates where the failure occurred.

Note:

Healthcheck verifies only installed services. It does not indicate if a service is not installed.

To run Healthcheck from a URL to check the status of web services

1. Ensure that the Healthcheck web.config file has been configured to the site's needs.
2. On the standalone station, launch Internet Explorer.
3. In the address bar, if Healthcheck has not been configured to automatically log in, type

   https://*fully_qualified_domain_name*/AgfaHC.Healthcheck.Escrow

   or

   If Healthcheck has been configured to automatically log in, type

   https://*fully_qualified_domain_name*/AgfaHC.Healthcheck.Escrow/EscrowForm.aspx

To	Append	Example
View the results in HTML	**?format=html** to the end of the URL	**https://appserver.hospital.com/AgfaHC.Healthcheck.Escrow/EscrowForm.aspx?format=html**
Add a refresh frequency	**?refresh=*seconds*** to the end of the URL	**https://appserver.hospital.com/AgfaHC.Healthcheck.Escrow/EscrowForm.aspx?refresh=60**
View the results in HTML and add a refresh frequency in the same URL	**?format=html&refresh=*seconds*** to the end of the URL	**https://appserver.hospital.com/AgfaHC.Healthcheck.Escrow/EscrowForm.aspx?format=html&refresh=60**

CAUTION!

Setting the refresh interval below five seconds impacts performance.

4. If Healthcheck has not been configured to automatically log in, type an IMPAX Administrator username and password, select the login domain, and click **Log in**.

   On the Agfa Web Services: Healthcheck page, all web services are listed with a status of Passed (green) or Failed (red) .

5. To determine what the problem is for any web services with the status Failed, review the **Comments**.
6. To check the status of the web services again, in Internet Explorer, click **Refresh**.

Transmitting studies from old standalone

(Topic number: 119794)

If you have installed the new standalone server as a replacement for an existing standalone that could not be upgraded due to hardware or operating system incompatibility, transmit studies from the old standalone station to the new one before deploying it.

Installing and configuring the IMPAX Client software

4

Complete the IMPAX Client software install tasks after installing and initially configuring the IMPAX Server and IMPAX Business Services software.

Important!

On a new standalone station, the IMPAX Client software is installed under Windows 7, the host operating system.

1. Installing and activating a Client license

(Topic number: 7678)

To run the IMPAX Client software, you must install and activate appropriate licenses for it. By following the procedures in *Creating the administration account* (refer to page 57), you have already set up an administration license. To set up other Client licenses that you receive from Agfa, use the License Manager Administrator Tool.

To install and activate a Client license

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **License Manager Administrator Tool**.

   The License Manager Administrator Tool is displayed in a command prompt window.

2. Ensure that you are at the **C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool** prompt.

3. At the prompt, type **almadmin -install *dir_name*\"*file_name*"**

where *dir_name* is the location of the file, and *file_name* is the file name of the license to be installed. For example, type **almadmin -install c:\temp\"0000001123-2.lic"**.

4. At the prompt, type **almadmin -activate *serialnumber-revisionNumber***

   where *serialnumber-revisionNumber* is the serial number of the license to be activated. For example, type **almadmin -activate 0001234567-2**. You can find the serial number in the license email.

5. To close the License Manager Administrator Tool, type **exit**.

2. Installing the IMPAX Client

(Topic number: 7776)

The following explains how to install IMPAX Client using the default InstallShield package. An alternative is to automate the installation through a batch file. For instructions on installing IMPAX Client that way, refer to "Enabling automated installation of the IMPAX Client software from a command prompt" (topic number 7802) in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

Note:

To install the IMPAX Client, you must be logged in as a user in a Administrators role that has permissions to the Windows Services.

To install the IMPAX Client

1. From the IMPAX Client CD or the IMPAX Client Installation web page (https://*install_server_name*/clientinstaller/*language_code*), start the IMPAX Client installation program, **IMPAXClientSetup.exe**.

   For information on setting up a Client installation server, refer to "Installing the IMPAX Installation Server" (topic number 7773) in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

   CAUTION!

   Do not use a standalone IMPAX workstation as an IMPAX Client Installer server. Instead, place the IMPAX Client Installer server program on another server.

2. If a File Download dialog appears, click **Open** or **Run**.

   A `Preparing to Install` message appears.

3. If a prompt appears about downloading and installing missing components, click **OK**.

4. Follow the prompts to download and install Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5 SP1, or all.

Note:

After installing a component, the installer may stop running or you may receive an `Installation is not yet complete` message. In either case, rerun the IMPAXClientSetup.exe program.

Depending on network speed, downloading and installing the Microsoft .NET Framework can take over 30 minutes.

For the .NET Framework 3.5 install, after the download, agree to the installation, accept the license agreement, and after the installation is complete click **OK**. If prompted, restart the computer.

If you do not have a live Internet connection, the downloading will not work. Instead, install the Microsoft .NET Framework 3.5 from the Client Installer server (https://*install_server_name*/clientinstaller/redist/dotnetfx35.exe).

For the .NET Framework 3.5 SP1 install, after the download, if prompted to start the installation, click **OK**. If prompted, restart the computer.

5. On the Welcome to the InstallShield Wizard for IMPAX Client screen, click **Next**.
6. On the License Agreement screen, read the license agreement. If you agree, select **I accept the terms in the license agreement**. Click **Next**.
7. To install the application into C:\Program Files\Agfa\IMPAX Client, on the Destination Folder screen, click **Next**.

   or

   To install the application to another location, click **Change**. In the Change Current Destination Folder dialog, browse for the directory location to install into and click **OK**. On the Destination Folder screen, click **Next**.
8. On the IMPAX Application Server screen, in the Get or confirm application server name field, type the fully qualified domain name of this standalone station. Click **Next**.

   A *fully qualified domain name* is the full name of a system, including its local host name and complete domain name. For example, if the standalone station is called *qastation*, it is on the network domain called *radnet*, and radnet is within the *healthorg.com* domain, the name to type would be *qastation.radnet.healthorg.com*.
9. On the IMPAX Login Type screen, select the appropriate authentication method: Windows, IMPAX, or Smart Card.
   - **Windows Authentication**—Logs into IMPAX using the Windows session credentials after launching the IMPAX Client or logging in with a Windows smart card.
   - **IMPAX Authentication**—Logs into the IMPAX Client separately from Windows. (If unsure of which option to select, use **IMPAX Authentication**.)
   - **Smart Card Authentication**—Logs into the IMPAX Client with a smart card in the **National Health Service (NHS) environment only**.
10. Click **Next**.

11. On the Ready to Install the Program screen, click **Install**.

    The program is installed.

12. On the InstallShield Wizard Completed screen, click **Finish**.

The IMPAX Client software is installed. You do *not* have to restart the computer.

3. Installing related Client software

(Topic number: 7661)

The following software packages can be integrated with the Client software. Which of these you need to install depends on who will be using the workstation, where the workstation is located (within or outside the network firewall), and what licenses are available at your site.

- **Voxar 3D**—Fully integrated application used for 3D, MPR, and MIP modeling and analysis.
- **Orthopaedic Application software**—Used for applying digital templates and completing measurements in preparation for orthopaedic surgery. This software is available on a separate installation CD and requires a hardware dongle.

For instructions on installing these software packages, refer to the topic "Installing related software" (topic number 7779) in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*

4. Installing paper printers

(Topic number: 7664)

The standalone station is armored. Armoring blocks all unused ports, including those that might be needed to add external devices such as paper printers. Therefore, before a paper printer can be installed, you must explicitly start the Print Spooler service.

To install paper printers

1. Open the Windows Administrative Tools.
2. Select **Services**.
3. From the Services list, right-click **Print Spooler** and select **Properties**.
4. In the Print Spooler Properties dialog, from the Startup type list, select **Automatic**.
5. Click **OK**.
6. From the Services list, right-click **Print Spooler** and select **Start**.
7. Close the Services and the Administrative Tools windows.
8. To add the paper printer, in Control Panel, select **Printers** and step through the wizard.

5. Adding IMPAX Client to the Startup menu

(Topic number: 7747)

On startup, the IMPAX Client performs some initial configuration tasks. If the user logs in before these tasks are completed, a delay occurs before the IMPAX Client window opens. To reduce this delay, add the IMPAX Client to the Windows Startup menu. This task is not required; it is an option for improving performance.

To add IMPAX Client to the Startup menu

1. Select **Start** > **All Programs**.
2. Go to **Agfa IMPAX** > **IMPAX Client**.
3. Right-click and drag **IMPAX Client** to the **Startup** menu.
4. Select **Copy Here**.
5. Confirm that you want to make this change for all users.

6. Renaming and assigning Client licenses

(Topic number: 7629)

Client license files have generic names that do not clearly identify their purpose. Use the License Manager Administrator Tool to give the license file a unique name that describes the role or abilities associated with this license. For example, the name can be changed to IMPAX Administrator or to Radiologist.

To rename and assign Client licenses

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **License Manager Administrator Tool**.
2. Ensure that you are at the **C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool** prompt.
3. At the prompt, type **almadmin -setAdminName *serial* "*name*"**

   where *serial* is the serial number of the license to be renamed and *name* is the new name for the license. For example, type **almadmin -setAdminName 1234567 "Entry Level Radiologist"**.
4. To close the License Manager Administrator Tool, type **exit** and press **Enter**.

   You can then assign licenses to roles in the Client. A role is collection of users or other roles that holds permissions and preferences as well as licensing options. For example, a role can represent the enterprise, the institution, a department, or a team.
5. In the IMPAX Client, assign the license to the appropriate roles.

   Refer to "Assigning licenses to roles" (topic number 9353) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Note:

When a license has been installed though the ALMadmin tool, then assigned to a role in the IMPAX Client, it may take up to 15 minutes before the users in that role can log into the system.

7. Completing other IMPAX Client configuration tasks

(Topic number: 7730)

When first implementing IMPAX at a site, the PACS Administrator must complete many other Client configuration tasks. These include:

- Configuring the workstation settings, including monitors
- Defining roles and users, including permissions and operations

  Operation defaults can differ between an install and upgrade of the Client. Check the settings for the operations to ensure the appropriate access to features is given.
- Creating and adding worklists
- Defining relevance rules for opening priors
- Setting hanging protocols for viewing studies (for radiologists)
- Configuring modality and body part preferences, including Image area tools
- Configuring DICOM printers and printing
- Readying image wizards and enabling preconfigured ones
- Defining the dictation workflow (for radiologists)
- Setting up logging of system activity

Information on how to complete these tasks is provided in the *IMPAX 6.5.1 Client Knowledge Base: Extended*, "Administering IMPAX" section (topic number 11588).

Troubleshooting IMPAX

A

As you install IMPAX servers, you may encounter various installation and configuration problems.

Troubleshooting: Installation of IMPAX software unsuccessful; must reinstall packages

(Topic number: 7685)

Issue

IMPAX Server was not installed successfully.

Details

If the IMPAX Server software installation was not successful, you may have to uninstall the IMPAX software and retry the IMPAX installation.

Solution

Before retrying the installation, attempt to determine why the installation failed and correct the problem, if possible. You can find specific error messages and more information on the installation in these log files:

- C:\mvf\data\logs\mitra_install.log
- C:\mvf\data\logs\build_mvf.log
- C:\mvf\data\logs\build-database.log
- C:\mvf\data\logs\add_impax_mvf.log

After the problem is determined and resolved, reinstalling the IMPAX software requires four steps:

1. Restart the system as indicated by the installer, even if failures have occurred.
2. Determine whether the security components were applied.

   If the installation failed after the security components were applied, you must log in using the AgfaService account to reinstall the IMPAX software. If the installation failed before the security components were applied, you must log in as a Windows administrator to reinstall the IMPAX software. Refer to the instructions that follow.
3. Uninstall the IMPAX software.
4. Install the IMPAX packages again, using the correct user account.

To uninstall the IMPAX software

1. Open Control Panel.
2. In Windows 2008, select **Programs and Features**.
3. Select **AGFA IMPAX AS300**.
4. Click **Change**.
5. At the prompt, type your name and click **Next**.
6. On the Welcome screen, select **Modify**. Click **Next**.
7. Clear the checkboxes of all installed packages. Click **Next**.
8. On the Maintenance Complete screen, select **Yes, I want to restart my computer now** and click **Finish**.

   Important!

   Do not manually delete the C:\mvf folder as part of the uninstall. If you do, you will have to re-create and reimport the portable password files.
9. Log into Windows as the AgfaService user.

You can then reinstall the IMPAX packages.

Troubleshooting: Web services do not run after installing or upgrading the Application Server

(Topic number: 118488)

Issue

After installing or upgrading the Application Server, web services do not start and applications such as the Configuration Tool do not run.

Details

During installation, InstallShield may have failed to install all the necessary files.

Solution

1. Check that all the expected files are present in the Web Services directory on the Application Server. Also check that the C:\Program Files\Agfa\Impax Business Services\Configurator directory is present and that this directory contains more than a few files.
2. If some of the files are missing from the Web Services directory, or if the C:\Program Files\Agfa\Impax Business Services\Configurator directory is missing or contains just a few files, run the Business Services installation program again and select the **Repair** option.
3. If the procedure you ran in the preceding step fails, uninstall (refer to page 86) and then reinstall the Application Server.

Important!

If you have to reinstall the Application Server, do not reinstall the ADAM or AD LDS database.

Troubleshooting: Application Server is unavailable after reinstalling IIS

(Topic number: 7743)

Issue

The Application Server is unavailable after IIS is uninstalled and reinstalled, and does not respond.

Details

The Microsoft Distributed Transaction Coordinator service must be running before IIS is reinstalled on a standalone station where the IMPAX Business Services component has already been installed.

To confirm the problem

1. Open the Windows Administrative Tools and select **Internet Information Services (IIS) Manager**.
2. Expand ***computer_name (local computer)*** > **Web Sites**.
3. Navigate to **Default Web Site** > **iisstart.asp**.
4. Right-click **iisstart.asp** and select **Browse**.

   If a problem exists, an Internal Server Error message is returned.

Solution

To determine whether IIS was reinstalled successfully

1. Open the Windows Administrative Tools and select **Component Services**.
2. Navigate to **Component Services** > **Computers** > **My Computer** > **COM+ Applications**.
3. Ensure that the following COM+ Applications are listed:

- IIS In-Process Application
- IIS Out-Of-Process Pooled Applications
- IIS Utilities

4. If the IIS applications are not listed, enable the Distributed Transaction Coordinator service and reinstall IIS.

To enable the Distributed Transaction Coordinator service

1. Open the Windows Administrative Tools and select **Services**.
2. Right-click **Distributed Transaction Coordinator** and select **Properties**.
3. On the General tab, from the Startup type list, select **Automatic**.
4. Click **Start**. Click **OK**.

Troubleshooting: Server license keys do not work

(Topic number: 7649)

Issue

Programs do not start because of Server license key problems.

Details

Server license keys can present problems if they are not stored in the correct directory or are not matched to the MAC addresses of the machines. To function properly, the correct number of license keys must be located in the correct directory.

Solution

Ensure that the appropriate license keys are installed in the correct location. Information on obtaining a MAC address is available in *Obtaining Server license keys* (refer to page 44).

To install the mvf license key

1. Match up the correct license key with the machine's MAC address.

   The license key name is the MAC address with a .lic file extension.
2. Open Windows Explorer.
3. Copy the license key file to the mvf directory on the hard drive.
4. Rename the license key file to **mvf.lic**.

Troubleshooting: Unsure whether certificates are installed

(Topic number: 7698)

Issue

Unsure whether certificates are installed.

Details

—

Solution

You can determine whether the certificates have been installed properly using the following steps.

To check whether any certificates are installed

1. Open the Windows Administrative Tools and select **Internet Information Services (IIS) Manager**.
2. Expand ***computername*** > **(local computer)** > **Web Sites**.
3. Right-click **Default Web Site** and select **Properties**.
4. Switch to the **Directory Security** tab.

   The installed certificate can be viewed using the **View Certificate** button. If the View Certificate button is disabled, no certificate is installed.

To use Console Management to check which certificates are installed

1. Open a command prompt.
2. Type **mmc**.
3. In the Console1 window, select **File** > **Add/Remove Snap-in**.
4. In the Add/Remove Snap-in dialog, click **Add**.
5. In the Add Standalone Snap-in dialog, from the list, select **Certificates**.
6. Click **Add**.
7. In the Certificates snap-in dialog, select **Computer account**. Click **Next**.
8. Click **Finish**.

   The certificate is added for the Computer account and appears in the list in the Add/Remove Snap-in dialog.
9. In the Add Standalone Snap-in dialog, click **Add** again.
10. In the Certificates snap-in dialog, select **Service account**. Click **Next**.
11. Click **Next** again.
12. From the Service account list, select **Agfa Healthcare**.

13. Click **Finish**.

    The certificate is added for the Service account and appears in the list in the Add/Remove Snap-in dialog.
14. In the Add Standalone Snap-in dialog, click **Close**.
15. Click **OK**.

To view whether the certificates are installed for the proper accounts

1. In the Console Root window, expand **Certificates (Local Computer)** > **Personal** > **Certificates**.

   On the right pane, the certificate should be issued to *machinename.fully_qualified_domain_name*.
2. On the left pane, expand **Trusted Root Certification Authorities** > **Certificates**.

   On the right pane, the certificate issued by the certificate authority should appear in the list.
3. Repeat steps 1 and 2 for **Certificates-Service (Agfa Healthcare)** > **ADAM_AgfaHealthcare\Personal** and **ADAM_AgfaHealthcare\Trusted Root Certification Authorities**.

Tip:

In case you ever need to check on installation again, in the Console window, choose **File** > **Save As** to save the certificates as an MSC file.

Troubleshooting: Cannot connect to the Administration Tools

(Topic number: 7740)

Issue

You cannot log into the Administration Tools.

Details

Two possibilities exist for this problem:

- The Administration Tools service can encounter service problems when you first attempt to log in.
- The IMPAX Server tries to communicate with the Administration Tools over the default port range of 1200-1270. If these ports are used up, the Server cannot reach the Administration Tools.

Solutions

If the login screen fails when it reaches 88%, this indicates a service problem. Stop and restart the Administration Tools service.

To stop and restart the Administration Tools service

1. Open the Windows Administrative Tools.
2. Select **Services**.
3. Right-click **Administration Tools Server** service and select **Restart**.

If ports 1200–1270 are used up, modify the default range to use a range that is available.

To modify the default port range

1. Open a command prompt.
2. To determine which ports are in use, type the following:

   netstat -a
3. Ports within the 1200-1270 range with a state of LISTENING do not have to be modified. If you find that the ports within that range do not have a state of LISTENING:
   a. In a text editor, open **C:\mvf\java\etc\jserver.properties**.
   b. Search for **jmtk.rmiPortRange=1200-1270**.
   c. Modify the range to suit the needs of the site.
   d. Save and close the modified file.

Troubleshooting: "Failed to load DLL: MtCmnSec" exception during AS300 server packages installation

(Topic number: 120619)

Issue

During the IMPAX 6.5.1 AS300 server packages installation, after typing your name and clicking **Next**, an exception occurs and the message `Failed to load DLL: MtCmnSec` is displayed.

Details

This exception could indicate that a different version of the LIBEAY32.dll file in the C:\windows\system32 directory is causing a version conflict.

Solution

1. Before closing the exception message, in Windows Explorer, search for the location of the MtCmnSec.dll that is used by the AS300 installer. The file is usually located in a directory under C:\Documents and Settings\Administrator\Local Settings\Temp\{*some_string*}\Disk1. For example:

   ```
   C:\Documents and Settings\Administrator\Local
   Settings\Temp\{61BCE0ED-5E0C-4A36-9F55-C23DAAB20C9D}\Disk1
   ```
2. Open a command prompt and change directories to the folder found in the previous step.
3. Type

rundll32 mtcmnsec.dll,mtGetWindowsVersion

An error similar to the following may appear:

```
The ordinal 3823 could not be located in the dynamic link library
LIBEAY32.dll
```

This error indicates that a different version of the LIBEAY32.dll file in the C:\windows\system32 directory is causing a version conflict.

4. Rename the copy in C:\windows\system32 and run the AS300 installer again.

Reinstalling Oracle on Windows

B

In rare circumstances, you may have to reinstall Oracle on Windows if you are experiencing problems that cannot be resolved by the usual troubleshooting techniques. This procedure describes how to reinstall Oracle on Windows.

Important!

This procedure is for reinstalling the same version of Oracle Server only. Do not use this procedure to upgrade to a newer Oracle version or patch set.

To reinstall Oracle on Windows

1. Remove the MVF and MVF_ORA ODBC System Data Source Names (DSNs).

   Using ORADIM, you must remove the MVF services if the AS300 software is to remain installed. This stops and removes the services in one step. For example, type

   delete oradim -DELETE -SID MVF

2. Navigate to the C:\oracle\product\10.2.0\db_1\database directory.
3. Make backup copies of the following files, if they exist:
   - initMVF.ora
   - PWDMVF.ora
   - SPFILEMVF.ora
4. Navigate to the C:\oracle\product\10.2.0\db_1\NETWORK\ADMIN directory.
5. Make backup copies of the following files, if they exist:
   - listener.ora
   - sqlnet.ora

- tnsnames.ora

CAUTION!

Serious problems might occur if you modify the registry incorrectly. These problems might require that you reinstall your operating system and there is no guarantee that these problems can be solved. We recommend that you back up the registry before you change it, so that you can back out the changes if necessary.

6. Select **Start** > **Oracle - ohome** > **Oracle Installation Products** > **Universal Installer**.
7. Select **Deinstall Products**.
8. Under Oracle Homes, select the **ohome** checkbox, then click **Remove**.
9. Click **Yes** to start the deinstallation.
10. When the deinstallation is done, restart the server, then log into Windows as an administrator-level user.
11. If the C:\oracle directory still exists, delete it.
12. If the C:\Program Files\oracle directory still exists, delete it.
13. Delete the registry key HKEY_LOCAL_MACHINE\Software\ORACLE.
14. If any files or directories reside in C:\cygwin\tmp, delete them.
15. Create a directory on the C:\ drive to store files that you will back up in the next step.
16. Move the C:\oracle_drives, C:\Oracle_install.log, and C:\installOracleInfo files into the directory you created in the previous step.
17. Restart the server, then log into Windows as an administrator-level user.
18. Use the OracleInstall package to install Oracle Server (refer to page 42).
19. After the installation finishes, copy the backup files you created in steps 3 and 5 into the original directories.
20. Re-create the MVF and MVF_ORA ODBC System Data Source Names (DSNs) as needed.

Note:

The AS300 installation automatically creates the MVF DSN.

Uninstalling IMPAX 6.5.1

C

If you encounter installation problems or need to redeploy the workstation, you may have to uninstall some of the IMPAX software.

Uninstalling IMPAX 6.5.1 Client

(Topic number: 7607)

The following procedure removes the IMPAX Client software, but not any integrated software (such as the Orthopaedic Application, TalkStation, or Voxar).

To uninstall IMPAX 6.5.1 Client

1. If the IMPAX Client is running, log out of it and close the Login window.
2. Open the Control Panel.
3. Select **Add or Remove Programs**.
4. Under Currently installed programs, select **IMPAX Client**.
5. Click **Remove**.
6. When asked to confirm the removal, click **Yes**.

A Preparing to remove dialog opens, then the IMPAX Client software is uninstalled.

Uninstalling IMPAX 6.5.1 Business Services

(Topic number: 7608)

If you must back out of an installation, or reinstall the IMPAX Business Services, use the following instructions.

To uninstall IMPAX 6.5.1 Business Services

1. Open Control Panel. Under Windows 2008, select **Programs and Features**.
2. Select any instance of **Agfa IMPAX Business Services 6.5.1** and click **Uninstall**.
3. Select **AD LDS Instance AgfaHealthcare** and click **Uninstall**.
4. Ensure that C:\Program Files\Agfa is empty.
5. Ensure that the AgfaHC virtual directories are removed. These directories are located wherever the web services were installed.

Uninstalling the IMPAX 6.5.1 documentation

(Topic number: 118482)

If required, you can uninstall the IMPAX 6.5.1 documentation.

To uninstall the IMPAX 6.5.1 documentation

1. Open Control Panel.
2. In Windows 2008, select **Programs and Features**.
3. In the Add or Remove Programs dialog, under Currently installed programs, select **AGFA IMPAX *version* Knowledge Base *buildnumber* Documentation**.
4. Click **Remove**.
5. In the confirmation dialog, click **OK**.

   A progress dialog appears as the documentation is uninstalled, giving the amount of time remaining. When the process is complete, the dialog closes.
6. Close the Add or Remove Programs dialog.

All installed IMPAX 6.5.1 documentation is uninstalled.

Uninstalling IMPAX 6.5.1 Server

(Topic number: 7605)

If you must back out of an installation or reinstall the IMPAX Server software, use the following instructions.

To uninstall IMPAX 6.5.1 Server

1. Open Control Panel.
2. Depending on the version of Windows, select **Add or Remove Programs** or **Programs and Features**.
3. Under Currently installed programs, select **AGFA IMPAX AS300**.

4. Click **Change**.
5. At the prompt, type your name and click **Next**.
6. At the Welcome dialog, select **Modify**. Click **Next**.
7. Clear the checkboxes of any AS300 packages to uninstall. Select the checkboxes of any packages to install.
8. Click **Next**.
9. In the Maintenance Complete dialog, select **Yes, I want to restart my computer now** and click **Finish**.
10. If no longer required on this server, you can also delete any Server license files stored in the C:\mvf directory.

External software licenses

D

Some of the software provided utilizes or includes software components licensed by third parties, who require disclosure of the following information about their copyright interests and/or licensing terms.

AutoFac 2.1.13

(Topic number: 121742)

Autofac IoC Container

Copyright (c) 2007-2008 Autofac Contributors

http://code.google.com/p/autofac/wiki/Contributing

Other software included in this distribution is owned and licensed separately, see the included license files for details.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Cygwin

(Topic number: 121758)

Copyright 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010 Red Hat, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print

or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

      The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so

that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Editline 1.2-cstr

(Topic number: 121768)

Flexgrid for .NET

(Topic number: 7695)

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Log4Net

(Topic number: 7648)

This product includes software developed by The Apache Software Foundation (http://www.apache.org/). Please read the LICENSE files present in the Help > About dialog of the IMPAX Client.

OpenSSL

(Topic number: 121771)

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*

==========

* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

*

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THEIMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*

==========

*

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

*

*This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA,

lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

*

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

*THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

*/

TCL 8.5.3

(Topic number: 121781)

This product includes software developed by The TCL Developer Xchange, and is subject to the following license:

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Xerces C++ Parser, version 1.2

(Topic number: 121761)

This product includes software developed by The Apache Software Foundation (http://www.apache.org/). Please read the LICENSE files present in the Help > About dialog of the IMPAX Client.

Zlib

(Topic number: 7595)

zlib.h -- interface of the 'zlib' general purpose compression library Version 1.2.1, November 17th, 2003

Copyright (C) 1995-2003 Jean-loup Gailly and Mark Adler

This software is provided “as-is”, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Glossary

A

AD LDS

Active Directory Lightweight Directory Service. Directory services for an individual application that controls user login and privilege information on Windows Server 2008. In an IMPAX installation, runs on the Application Server.

APIP

Agfa Proprietary Imaging Protocol. Used to receive the proprietary format, reformat the images to DICOM and redirect them to the SCP. An APIP SCP is used specifically to receive images from certain older Agfa image sources.

Autopilot

Service that removes old and expired data when the cache starts to get full. This maintenance function keeps the database to a manageable size.

C

cc objects

Change Context (cc) objects are DICOM objects used to communicate and synchronize study metadata changes across multiple IMPAX clusters.

compression

Reduces the size of a file to save both file space and transmission time. Lossless, lossy, and wavelet are examples of compression types.

Curator

Curator is an IMPAX MVF server component. It is responsible for compressing incoming images into the Mitra Wavelet format and storing them in the web cache. These studies can be accessed by remote or local clients.

D

database

A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

diagnostic monitor

High-quality, grayscale monitors in sizes ranging from 1.3 to 5 MegaPixels, with either a portrait or landscape orientation.

DICOM

Digital Imaging and Communications in Medicine. The standard communication protocol used by a PACS, HIS, or modality to exchange information or images with other systems.

F

firewall

On a local area network (LAN) connected to a larger network, the security system that prevents outside intrusion and that keeps internal information from getting out. Typically, all traffic must pass through the machine on which the firewall is implemented.

fully qualified domain name (FQDN)

The full name of a system, consisting of its local host name and its domain name, including a top-level domain. For example, venera is a host name and venera.isi.edu is a fully qualified domain name. A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called name resolution, uses the Domain Name System (DNS).

H

hardware dongle

A device that attaches to a computer to control access to a particular application. Dongles provide the most effective means of copy protection. Typically, the dongle attaches to a PC's USB port.

high availability

With a high-availability solution, a site is protected against system downtimes, either planned or unplanned. Redundant servers are put in place that can take over functionality should the primary server become unavailable.

HSM

Hierarchical Storage Management. An HSM archive system provides long-term storage of data and access to data. Studies archived with HSM are stored to a file system. A mount point and subdirectory to store studies to is specified. The HSM system handles data storage.

HTTPS

Hypertext transfer protocol, secure, a URL access method for connecting to http servers using SSL (secure sockets layer).

I

IP address

The Internet Protocol address is a numeric address that identifies the station to other TCP/IP devices on the network.

L

license, IMPAX Client

IMPAX Client licenses define which IMPAX features users in a role can be given permission to access. They include standard and optional features. IMPAX Client license files are installed on Application Servers and are assigned to roles.

logical volume

Pooled logical extents can be concatenated together into virtual disk partitions called logical volumes or LVs. Systems can use LVs as raw block devices just like disk partitions: creating mountable file systems on them, or using them as swap storage. In computer storage, logical volume management provides a method of allocating space on mass-storage devices that is more flexible than conventional partitioning schemes.

M

MAC address

Media Access Control address. The unique physical address of each device's network interface card.

MIP

Maximum Intensity Projection. Refers to a projection of the 3D object that shows the tissues of highest density.

modality

An imaging discipline, such as CT, or a device that gathers digital information, such as digitizers for X-ray film, MRI scanners, and CR devices.

MPR

Multi-Planar Reformatting. A method of visualization in three-dimensional medical imaging. This method allows you to view anatomy along its central axis, or perpendicularly to that central axis.

MVF_SCU

A process that handles store and retrieve jobs for the PACS Store and Remember archive.

On IMPAX systems, it runs on the Network Gateway.

N

network

A group of computers, peripherals, or other equipment connected to one another for the purpose of passing information and sharing resources. Networks can be local or remote.

Network Gateway

The Network Gateway is part of the IMPAX MVF cluster. Essentially, this is the workflow manager of the IMPAX 6.0 and later system. The Network Gateway controls the studies coming into the cluster from an acquisition station, validates these incoming studies against information from the HIS or RIS, and routes the validated studies to cache or archive.

O

OCR

Optical Character Recognition is the recognition of printed or written characters by a computer. If a modality generates images into the system but not enough information about a study is sent, OCR templates read information directly from the burned demographics.

operations, IMPAX

The IMPAX actions allowed by a permission. For example, operations include dictation, printing to paper, and executing SQL statements through CLUI. You can further refine some operations by setting a study status flag on the operation. For example, you can allow printing only on dictated studies.

Orthopaedic Application

Application integrated with the IMPAX Client, used to do pre-surgical and postoperative planning for orthopaedics.

P

PACS

A Picture Archive and Communication Systems (PACS) makes it possible to electronically store, manage, distribute, and view images.

PAP

PACS Archive Provider. A PACS Archive Provider (PAP) acts like a Service Class Provider (SCP) in that it receives studies. However, it differs from an SCP in that the PAP can automatically register a study as PACS archived if the study originates from a source that the PACS stores to and remembers from, without having to queue the study for archiving back to the source. The PAP can also parse the private tags of the incoming DICOM

objects to determine HIS verification and study status.

permissions, IMPAX

Permissions define the available IMPAX features and types of studies that users in a particular role have access to. Permissions are made up of a set of operations.

S

SCP

Service Class Provider. A DICOM server that receives requests from an SCU. The DICOM SCP accepts images for processing, processes find and retrieve requests, and handles storage commitment requests and replies.

SCU

Service Class User. Primarily sends DICOM requests to an SCP.

site

A type of resource, referring to the overall hospital facility that houses departments, locations, specialties, and stations.

SSL certificate

A digital certificate with the SSL protocol that has been issued by a certificate authority.

stations

Within the context of the IMPAX Client configuration interface, refers to a computer that has the IMPAX Client installed. Stations can be in a radiology reading room, in the offices of clinicians, or in the homes of radiologists, for example. When a user logs into IMPAX for the first time, the computer name is listed in the navigation pane of the Configure area - Stations section. Stations are organized under station containers. You can set configuration options, such as diagnostic monitor settings, memory usage, and so on, for a specific station, or the station can inherit its configuration from the station container.

U

UNC

Universal Naming Convention. A convention for identifying servers and other resources on a network. UNC uses the format *servername**resource*.

W

workflow

A sequence of events, initiated by a trigger event.

worklist

A collection of patients and their studies. For radiologists, the worklist is analogous to a pile of film jackets. They use the worklist to know which studies they must interpret during a specific time period. For technologists, a worklist is a list of the studies they must perform at specific times for each patient.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z