Application Server Installation, Upgrade and Configuration Guide

IMPAX 6.5.1

Detailed Instructions for Installing and Configuring the Application Server

AGFA

see more | do more

Copyright information

Trademark credits

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.

The information in this publication is subject to change without notice.

2011 - 6 - 15

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.
- No software other than that which is distributed with this package or is sanctioned by Agfa will reside on the IMPAX 6.5.1 computers.

Additional documentation

(Topic number: 11330)

This guide is intended for service and administrator personnel who are configuring IMPAX 6.5.1. It provides information about the required components and instructions for the configuration.

Details concerning installation of IMPAX are provided through this guide. Additional configuration information is available in the *IMPAX 6.5.1 Application Server Knowledge Base*.

To open the *IMPAX 6.5.1 Application Server Knowledge Base*

1. Ensure the documentation has been installed.

   For instructions, refer to *Installing the IMPAX documentation (refer to page 145)*.
2. Double-click the IMPAX 6.5.1 Knowledge Base desktop icon.

To open the *IMPAX 6.5.1 Application Server Knowledge Base* from the **Business Services Configuration Tool**

1. Ensure the documentation has been installed.

   For instructions, refer to *Installing the IMPAX documentation* (refer to page 145).
2. From the **Start** menu, select **Programs** > **Agfa HealthCare** > **Business Services** > **Configuration Tool**.
3. In the Business Services Configuration Tool, click **Help**.

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

What is the Application Server?

(Topic number: 11131)

The Application Server is the middle tier server which contains business logic and services for the communication between the IMPAX Clients and servers. It replaces direct connections to server components by acting as a proxy and providing services, such as user authentication, to Clients. Because the Application Server can be exposed outside of the firewall, the security of the Application Server is important to ensure the security of the cluster and the rest of the network.

The following tools are installed on the Application Server:

- **Business Services Configuration Tool**—Use the Configuration Tool to set up connections to the database, auditing server. The Business Services Configuration Tool controls logging levels for the web services and establishes the connection to the ADAM and AD LDS database servers as well as messaging servers.
- **License Manager Administration Tool**—Licensing on the IMPAX Client is assigned according to roles. The licenses that a user can access are inherited from the roles in which a user is a member. Use the License Manager Administrator Tool to install, activate, and rename the licenses that are available for the IMPAX Client roles.
- **Security Wizard**—Use the Security Wizard to install and generate requests for SSL certificates, manage web services, and create administration accounts for IMPAX.
- **ImpaxAdam**—Use ImpaxAdam to update, remove or reinstall an existing ADAM AgfaHealthcare instance, to display diagnostic information about ADAM, and to manage dual-cluster hosts.

IMPAX cluster overview

(Topic number: 7791)

Every IMPAX installation is based on the following main components:

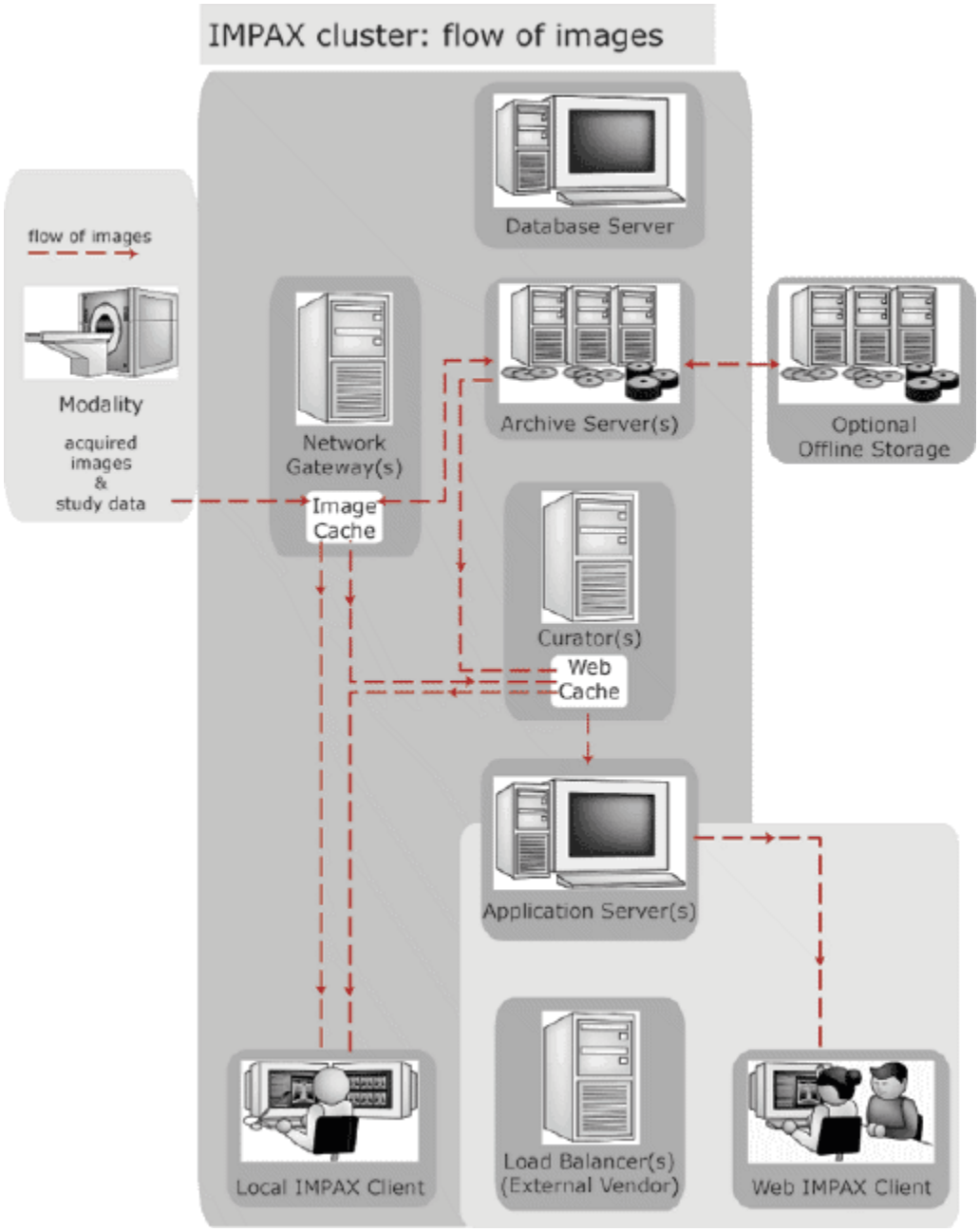
- Network Gateway
- Archive Servers
- Oracle Server or SQL Server
- Application Server
- Curator
- IMPAX Clients—local and remote

The sum of these components is called the *cluster*. An IMPAX cluster is the set of core IMPAX components that contains one database. SPFTP/ASPFTP is used for communication within the IMPAX cluster. Any third-party display stations are considered to be outside the cluster. They use DICOM to communicate with the cluster.

A typical installation has a Database Server, one or more Archive Servers, one or more Network Gateways, and one or more Curators. A third-party load balancer is optional, to help handle many Clients. Local Clients are spread throughout the entire enterprise, and remote Clients outside the enterprise firewall. These Clients connect to one or more Application Server machines, either directly or through a load balancer. The Application Server acts much like a proxy machine to handle security, authentication, and communication with the IMPAX Server components.

When images are transmitted to the IMPAX cluster, the Network Gateway performs validation of the study images and data. Validation requires the Network Gateway to query the HIS/RIS and ensure that the study and patient demographics match what is currently incoming from a modality or a transmit device. If the validation is successful, the images are "allowed" into the system. The Database Server collects and manages all patient and study demographic data.

The IMPAX Clients, both local and remote, are used to view study images. Local Clients can get images directly from the Network Gateway image cache. If images have been archived, the Network Gateway image cache gets them from the Archive Server. The Curator generates compressed wavelet images and stores them in a web cache, which may also be seen by local Clients. When a study is diagnosed and dictated, the status of the study is updated at the Database Server, and when a report is generated, it is forwarded to the HIS/RIS.



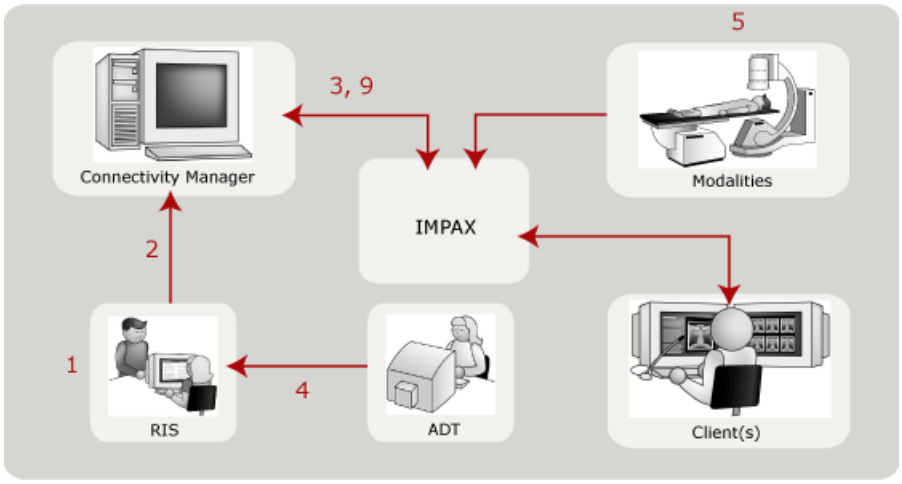
Deploying IMPAX as a data center with IMPAX spokes

(Topic number: 11647)

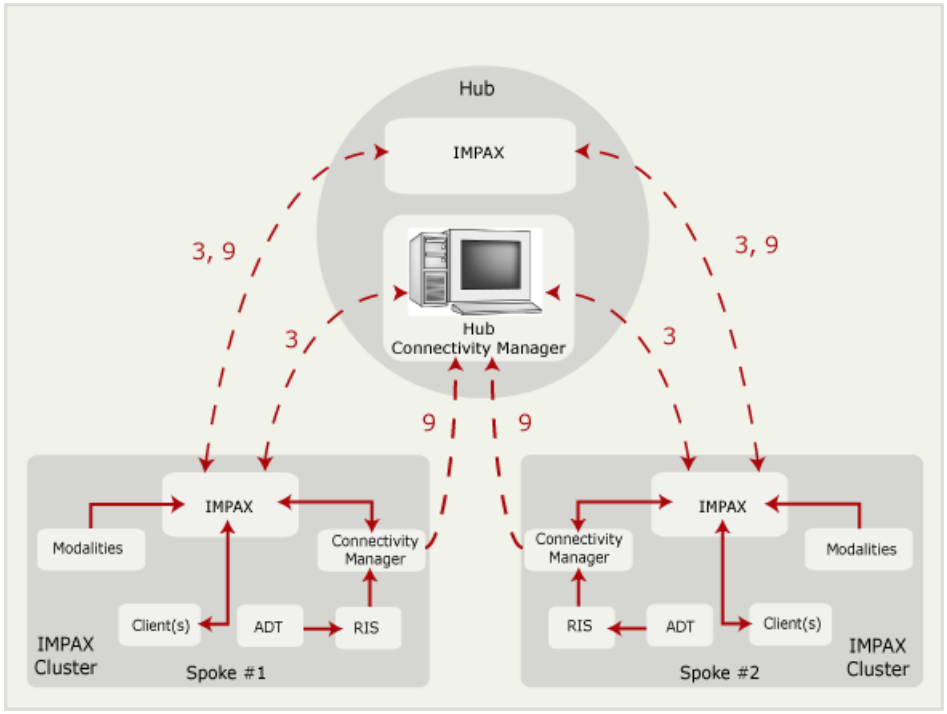
One IMPAX cluster can be set up as central repository (or hub) for archiving studies from several individual IMPAX clusters, called *spokes*. This way different sites can share studies while not each

having to maintain an extensive archive on-site. The hub IMPAX cluster acts as a *data center* for the spokes.

Single cluster



Multiple clusters



1. A study is scheduled for a patient and the details are recorded in the RIS. The study is scheduled well in advance of the actual appointment, but the order may not be recorded in the RIS until the day before the exam.
2. The RIS sends the order to the IMPAX Connectivity Manager, using an HL7 notification.

3. The night before the scheduled study, the Connectivity Manager sends IMPAX notification of the study and IMPAX automatically searches for and retrieves relevant priors images from the local archive. This process is called *prefetching*.

   If the facility is part of an enterprise or a multiple IMPAX cluster installation, IMPAX also searches for relevant priors in the long-term or central storage data center.

4. The patient arrives and needs to be admitted to the facility to have a study performed. The system checks the ADT to see if a record already exists for the patient. If so, that patient ID is used; otherwise, a new patient ID is generated.
5. The study is performed on a modality and is sent to the local IMPAX cluster.
6. HIS verification is performed on the patient demographics of the study.
7. When IMPAX receives the study, it checks to see if it needs to get relevant priors from the local archive and fetches them. This process is called *autofetching*. It generally occurs when prefetching cannot be performed or when studies have been added to the archive.

   In an enterprise installation, the search includes priors stored in the data center.

8. When the radiologist completes the report, it is sent to the Connectivity Manager.
9. The Connectivity Manager sends the report to the Application Server, where it is forwarded to the IMPAX archive for storage. If the RIS is an IMPAX RIS or a queryable one, the report is stored on the RIS.

   In an enterprise installation, the Connectivity Manager also sends the completed report to the data center's Connectivity Manager, using HL7. At this point, the study will also be sent to the data center.

Order of cluster installations

(Topic number: 7763)

The IMPAX cluster has many components and each depends on other components in the cluster. To correctly install and configure components in the cluster, follow this order of installation:

1. **Install the Database Server, Archive Server, and Network Gateway.**

   Install the core Server components and create the portable password file required to install other IMPAX components. Do not configure the AS300 Server components at this time; the Application Server must be installed before these Server components can be configured. Refer to the guide appropriate to your configuration.

   Required guide: One of *IMPAX 6.5.1 AS3000 Installation and Configuration Guide* or *IMPAX 6.5.1 AS300 Installation and Configuration Guide*

2. **Install the Application Server.**

   Install the Business Application services and IMPAX documentation on the Application Server.

   Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

3. **Begin configuration of the Application Server.**

Create and import an SSL certificate, configure ADAM (Windows Server 2003) or AD LDS (Windows Server 2008), compress web services, set connections to the image and audit servers, and set logging levels.

Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

4. **If you have installed a Windows-based Database Server, Archive Server, or Network Gateway, configure these components.**

   Configure database backups, image and web caches, and archives (if necessary). In clusters that include only Solaris-based systems, these configuration steps are done automatically during the installation.

   Required guide: *IMPAX 6.5.1 AS300 Installation and Configuration Guide*

5. **Install and configure Curator and the CD Export server.**

   If the site requires compressed web images, install and configure one or more Curator systems and set up the web cache. If you are installing multiple Curators, install and start the master Curator first, then install and start the slave Curators.

   If you will be using the CD Export feature in the IMPAX Client, install the CD Export server.

   Required guide: *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*

6. **Complete the configuration of the Application Server.**

   Complete the optional Application Server configuration tasks that are applicable to the site.

   Required guide: *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*

7. **Install and configure Clients.**

   Install and configure the IMPAX Client, the PACS system used to access images.

   Required guide: *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*

If installing a standalone station (single-host AS300 with Application Server and Client), refer to the *IMPAX 6.5.1 Standalone Installation and Configuration Guide*.

If installing a single-server (single-host AS300 with Connectivity Manager and Application Server), consult *Installing an IMPAX AS300 single-server* (refer to page 152) in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

All documentation is available on the IMPAX Documentation DVD.

What is the IMPAX Enterprise Solution?

(Topic number: 56712)

The IMPAX Enterprise Solution is an integrated offering designed to meet the needs of large healthcare organizations. The IMPAX Enterprise Solution:

- Leverages the diversity and depth of the Agfa IMPAX product portfolio
- Forms an integrated solution for large-scale healthcare institutions with multi-disciplinary and multi-departmental needs

- Delivers consistent and predictable workflow and outcomes, employing workflow-aware adaptability and scalability

Key modules in the IMPAX Enterprise Solution

The foundations of the IMPAX Enterprise Solution are the key modules in a fully integrated offering:

- PACS
- RIS
- Reporting

Integrating into the IMPAX Enterprise Solution

(Topic number: 56715)

As part of the IMPAX Enterprise Solution, this product must be configured to fully support an integrated RIS-PACS-Reporting solution. For details about planning and implementing a RIS-PACS-Reporting integration, contact your local Agfa representative.

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.

You can install the IMPAX Application Server at any time when setting up the IMPAX system, but you must configure the Application Server after the IMPAX Server machines, including the database, are installed and configured.

IMPAX Application Server hardware and software requirements

(Topic number: 6682)

The following lists the hardware and software requirements for an Application Server. Where a specific manufacturer is identified, only that manufacturer's device is supported.

IMPAX Application Server: Hardware requirements

(Topic number: 6691)

The following hardware configuration is recommended for Application Servers.

Important!

When installing or upgrading to IMPAX 6.5.1 on Windows machines, all IMPAX Clients, Servers, and Application Servers must have Pentium 4 or later CPUs. CPUs earlier than Pentium 4 do not support the SSE2 instruction set required for FIPS-compliant versions of the OpenSSL library used for authentication, encryption, and decryption.

Component	Requirements
System	**Preferred:** HP ML370 G6/G7, DL380 G6/G7 **Supported:** Dell 1900, 2900, 2950, 6900*, 6950* Stratus Ft 4300, 4410, or 5700 (dual CPU)**
CPU	Minimum: 1 x dual core
RAM	2 GB minimum
Hard drive space	2 x 73 GB (Mirrored)
RAID	Embedded
Tape backup	DAT 72 tape drive (if required for backup)
Modem	N/A
DVD-ROM	Yes
Network interfaces	100/1000 Mbps
Video	KVM Integrated video
Power supplied	Redundant
Peripherals	KVM or mouse and keyboard

* The use of four-CPU socket servers for IMPAX is supported but not recommended.

** Stratus Servers are no longer supported for new installs.

IMPAX Application Server: Software requirements

(Topic number: 6621)

The following tables list the required software for Application Servers using Windows Server 2003® and Windows Server 2008® platforms. Unless otherwise indicated, Agfa does not provide the software as part of the Application Server installation package.

Component	Requirements
Operating system	Windows Server 2003® R2 SP2, Standard or Enterprise Editions 32 bit Windows Server 2008® SP2, Standard or Enterprise Editions 32 bit

Component	Requirements
Remote access	Symantec pcAnywhere™ version 12.5
Other explicit software	• IIS 6.0 for Windows 2003 R2 Server IIS 7.0 for Windows 2008 SP2 • Microsoft Internet Explorer 7.0 or 8.0 • LDAP—ADAM SP1 services (Windows 2003 Server) AD LDS (Windows 2008) • Java 1.6 • .NET 3.5 SP1 • Latest version of Adobe® Reader® • Norton Antivirus 6.1 or higher, Trend Micro, McAfee Antivirus 4.5 or higher
Database connection software	If connecting to an Oracle database: • Oracle 10g Client Release 2 (10.2.0.4.0) for Microsoft Windows (32-bit)—Oracle .NET Data Provider If connecting to a SQL Server database: • Integrated MDAC, which is included in the installation of the Application Server Business Services or SQL Server 2005 SQL Native Client

Installation preparation checklist

(Topic number: 11230)

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

Required installation information	Notes
If installing on a Dell, a separate computer already running Windows and a CD-ROM drive are required.	
Drive letter of the CD-ROM drive (typically D)	
Organization name	
Fully qualified domain name of the computer	
Administration user ID and password	
Appropriate regional settings	

Required installation information	Notes
Whether the network setup is Workgroup or Domain	
Type of database the Application Server is connecting to—Oracle or Microsoft SQL Server 2005/Microsoft SQL Server 2008.	
Obtain an IMPAX 6.5.1 Administrator 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.

Installing external software

2

Follow the instructions for installing external software applications for the Application Server.

External software: Order of installation tasks

(Topic number: 11238)

You must install and configure the software on the Application Server in the order it is listed. For more information on installing the required external software, refer to the documentation provided with the software or consult the vendor's website.

Note:

If connecting to a SQL Server Database Server, you do not have to install the Oracle 10g Client.

Windows Server 2003

Order	Installation or configuration task
1	*Installing Windows Server 2003* (refer to page 23)
2	*Upgrading Windows Server 2003 to Windows Server 2003 SP2* (refer to page 24)
3	*Setting the primary DNS suffix* (refer to page 33)
4	*Configuring Windows Server 2003* (refer to page 26)
5	*Switching to Control Panel classic view for Windows 2003* (refer to page 27)
6	*Partitioning disks on the Application Server on Windows 2003* (refer to page 28)

Order	Installation or configuration task
7	*Installing IIS 6.0 on Windows 2003* (refer to page 29)
8	*Installing ASP.NET* (refer to page 31)
9	*Installing and configuring pcAnywhere 12.5* (refer to page 42)
10	*Installing and configuring the Oracle 10g Client for Windows* (refer to page 132)
11	*Installing and configuring antivirus software* (refer to page 45)
12	*Installing Adobe Reader* (refer to page 45)

Windows Server 2008

Order	Installation or configuration task
1	*Installing Windows Server 2008* (refer to page 32)
2	*Setting the primary DNS suffix* (refer to page 33)
3	*Configuring Windows Server 2008* (refer to page 34)
4	*Upgrading Windows Server 2008 to Windows Server 2008 SP2* (refer to page 37)
5	*Partitioning disks on the Application Server on Windows 2008* (refer to page 38)
6	*Adding roles and role services in Windows 2008* (refer to page 39)
7	*Configuring IIS logging* (refer to page 40)
8	Installing AD LDS
9	*Installing and configuring pcAnywhere 12.5* (refer to page 42)
10	*Installing and configuring the Oracle 10g Client for Windows* (refer to page 132)
11	*Installing and configuring antivirus software* (refer to page 45)
12	*Installing Adobe Reader* (refer to page 45)

General installation notes for installing external software

(Topic number: 7061)

Restart the computer whenever any installation package asks you to do so. For instance, during the restart at the end of the Windows Server 2003 or Windows Server 2008 installation, the installation process registers files with Windows and replaces some files. For your installation to work properly,

make sure that if you are asked to restart during the install, you do so before proceeding to the next step.

Installing and configuring Windows Server 2003 SP2

(Topic number: 98108)

Follow these instructions to install and configure Microsoft Windows Server 2003 SP2.

Installing Windows Server 2003

(Topic number: 9883)

Before you begin the Windows installation, ensure that the proper CD drivers are installed.

Important!

If you are using RAID, be sure to configure it before installing Windows Server 2003.

To install Windows Server 2003

1. On the Welcome screen, press **Enter**.
2. To accept the license agreement, press **F8**.
3. To create a partition, press **C**.
4. If intending to install Oracle on Windows or Microsoft SQL Server on this server, set the partition size to 73 GB and press **Enter**.

   Note:

   Application servers have different partitioning requirements. For Application servers, set the partition size to 40 GB.

   .
5. To set up Windows on the partition, press **Enter**.
6. 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.
7. Follow the setup wizard using the following selections:

Option	Selection
Name	**Agfa**

Option	Selection
Organization	**Agfa**
Product Key	Windows ID number
License Mode	**Per Server** licensing, **5** licenses
Computer Name	As specified on order The maximum length for the host name is 16 characters. **Important!** To support database communication, you must enter the Computer Name in all uppercase letters.
Network Setting	**Typical** or as per the network administration policy
Workgroup/Domain	Select the **Workgroup** option, unless the computer will be connecting to the hospital domain for authentication. In that case, select **Domain**. Workgroup name is **IMPAX**.

8. When CD 1 installation is complete, restart the server.
9. When prompted, insert Windows Server 2003 CD 2.
10. When CD 2 installation is complete, restart the server.
11. Install the latest Windows Update patches.

Upgrading Windows Server 2003 to Windows Server 2003 SP2

(Topic number: 47207)

If the server that you are upgrading or installing is running Windows Server 2003 or Windows Server 2003 Service Pack 1, we recommend that you install Microsoft Windows Server 2003 Service Pack 2.

CAUTION!

This topic provides only basic upgrade instructions. For complete installation instructions, refer to the applicable topics in the Microsoft Server 2003 Technical Library, including the *Windows Server 2003 Service Pack 2 Installation and Deployment Guide*.

You can install SP2 from the SP2 CD or from the Web. The installation file is named WindowsServer2003-KB914961-SP2-*XXX*-*LLL*.exe, where *XXX* stands for the type of operating system (for example, x86) and *LLL* stands for the language (for example, ENU).

To upgrade Windows Server 2003 to Window Server 2003 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 WindowsServer2003-KB914961-SP2-*XXX-LLL*.exe into the distribution folder.
4. Open a command prompt.
5. To extract the files, type the following:

   WindowsServer2003-KB914961-SP2-*XXX-LLL*.exe /X:[***Path***]

   If the distribution folder is local, you do not have to specify the path.
6. To install the service pack from a remote shared distribution folder, run **Update.exe**.

   If the distribution folder is local, Update.exe starts automatically.
7. Follow the instructions in the Setup Wizard.
8. When the installation process is complete, restart the computer.

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

Setting the primary DNS suffix

(Topic number: 7621)

Note:

This topic applies to Windows Server 2003 and Windows Server 2008.

When referring to the server running the IMPAX Business Services, 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

1. On Windows Server 2003, right-click **My Computer** and select **Properties**.

   or

   On Windows Server 2008, right-click **Computer** and select **Properties**.
2. If the operating system is Windows 2003, skip this step. On Windows Server 2008, click **Advanced System 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.
9. Log into Windows as an administrator-level user.

Configuring Windows Server 2003

(Topic number: 47531)

To configure Windows Server 2003, complete the following tasks.

Activating Windows 2003

(Topic number: 47537)

Windows Server 2003 must be initially activated.

To activate Windows 2003

1. If you have not already activated Windows Server 2003, select **Start** > **All Programs** > **Activate Windows**.
2. Follow the on-screen prompts.

Changing the paging file setting in Windows 2003

(Topic number: 59229)

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

To change the paging file setting in Windows 2003

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

   Set a value that is 1.5 to 2 times the size of the physical memory. For example, if the computer has 2 GB of RAM, set the Initial size to 4096.
8. In the Maximum size (MB) field, type the **same** value entered in the Initial size field.
9. Click **SET**.

10. Click **OK**.
11. Restart the computer.

Overwriting Windows events as necessary

(Topic number: 47540)

IMPAX functions better when Windows events are overwritten as needed.

To overwrite Windows events as necessary

1. Open the Windows Administrative Tools and select **Event Viewer**.
2. Complete the following steps for each log under Windows logs and Application and Services logs in the Event Viewer:
    a. Right-click the log and select **Properties**.
    b. Under Log Size, select **Overwrite events as needed**. Click **OK**.

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, folders and drives.**.
5. Clear the **Hide extensions for known file types** checkbox.
6. To save the changes, click **OK**.

Switching to Control Panel classic view for Windows 2003

(Topic number: 7716)

Windows 2003 Server can be configured to use different Control Panel categories than previous releases of Windows. To follow the procedures in this guide, the Control Panel should be displayed with the classic Windows categories instead.

Note:

By default, the Control Panel in Windows 2003 Server is displayed in classic view.

To switch to Control Panel classic view for Windows 2003

1. Open Control Panel.

2. In the left pane, under Control Panel, select **Classic View**.

   The Control Panel window refreshes to display the same categories as in older releases of Windows. In the left pane, **Icon View** is displayed under the Control Panel heading.

Creating a temporary directory
(Topic number: 47571)

Having a temporary directory on the server can be useful for storing files in the short term.

To create a temporary directory

1. In Windows Explorer, select the **C:** drive.
2. Select **File** > **New** > **Folder**.
3. Rename the new folder as **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.

Partitioning disks on the Application Server on Windows 2003
(Topic number: 11206)

We recommend partitioning the disks on the Application Server as described in this procedure. For security and performance reasons, we recommend that the Web Services that are installed with the IMPAX Business Services be placed on a drive other than C.

Recommended partition sizes

We recommend that you create the following disk partitions

Partition	Size
C:\	40 GB
E: WebServices	5–10 GB

Partition	Size
L: Logs	Rest
R: Recovery	20 GB

To partition disks on the Application Server on Windows 2003

1. From the **Start** menu, select **Administrative Tools** > **Computer Management**
2. Under Storage, select **Disk Management**.
3. Right-click the unallocated disk you want to format and select **New Partition**.
4. In the wizard, click **Next**.
5. Select **Extended Partition** and click **Next**.
6. Accept all the space and click **Next**, then click **OK**.
7. Right-click the green Free Space you just created and select **New Logical Drive**.
8. In the wizard, click **Next** until you reach the screen for assigning a drive letter.
9. From the **Assign the following drive letter list**, select the drive using the table above for drive names and letters.
10. Click **Next**.
11. Set the following variables:
    - File System to **NTFS**.
    - Volume Label to WEBSERVICES - see the table above for drive names and letters..
    - Format Options to **Quick Format**.
12. Click **OK**.

    The partition is formatted.
13. Exit Disk Management.

Installing IIS 6.0 on Windows 2003

(Topic number: 7670)

The Application Server requires IIS, as do the Administration Tools and the Knowledge Base.

CAUTION!

When installing IIS, ensure that you do not install the remote administration options, as these pose a security risk.

To install IIS 6.0 on Windows 2003

1. Open Control Panel.
2. Select **Add or Remove Programs**.

3. Click **Add/Remove Windows Components**.
4. In the Windows Components Wizard dialog, select the **Application Server** checkbox.
5. Click **Details**.
6. Select **Internet Information Services** and click **Details**.
7. In the Internet Information Services (IIS) dialog, select the **World Wide Web Service** checkbox.

   The Internet Information Services Manager and Common Files checkboxes are automatically selected.
8. Click **OK** until you return to the Windows Components Wizard dialog.
9. To install IIS, click **Next**.
10. To close the installation wizard, click **Finish**.

Configuring IIS logging

(Topic number: 116031)

On Windows 2003 and Windows 2008 Application 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 2003 Application Server

(Topic number: 60133)

IIS logging is enabled by default, 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 situation, disable IIS logging.

Tip:

If you prefer to keep IIS logging active, change the location of the IIS log files (refer to page 30).

To disable IIS logging on a Windows 2003 Application Server

1. Right-click **My Computer** and select **Manage**.
2. In the Computer Management window, navigate to **Services and Applications** > **Internet Information Services (IIS) Manager** > **Web Sites** > **Default Web Site**.
3. Right-click **Default Web Site** and select **Properties**.
4. In the Default Web Site Properties dialog, clear the **Enable logging** checkbox.
5. Click **OK**.

   IIS logging is disabled.

Changing the location of the IIS log files on a Windows 2003 Application Server

(Topic number: 60163)

IIS logging is enabled by default, 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. If you prefer not to

disable IIS logging (refer to page 30), you can prevent this situation by saving the log files in a different location.

To change the location of the IIS log files on a Windows 2003 Application Server

1. Right-click **My Computer** and select **Manage**.
2. In the Computer Management window, navigate to **Services and Applications** > **Internet Information Services (IIS) Manager** > **Web Sites** > **Default Web Site**.
3. Right-click **Default Web Site** and select **Properties**.
4. In the Default Web Site Properties dialog, in the Enable logging section, click **Properties**.
5. In the Log file directory field, type the directory for the log files.

   Specify a directory path, on a drive other than C:, with significant free space.
6. Click **OK**.

   Log files are now saved in the new location.

Installing ASP.NET

(Topic number: 7672)

ASP.NET is required before installing the IMPAX Business Services.

Note:

These instructions apply to Windows 2003 only. If you are configuring a machine with Windows XP, or Windows 2008, proceed with the next task.

To install ASP.NET

1. Open Control Panel.
2. Select **Add or Remove Programs**.
3. In the Add or Remove Programs dialog, click **Add/Remove Windows Components**.
4. In the Windows Components Wizard dialog, select the **Application Server** checkbox.
5. Click **Details**.
6. To select the .NET provider, select the **ASP.NET** checkbox.
7. Click **Next**.
8. If prompted, insert the Windows 2003 CD or provide a path to the Windows 2003 installation files.
9. When the Windows Components wizard has finished configuring Windows Server 2003, click **Finish**.

Installing and configuring Windows Server 2008

(Topic number: 98105)

Follow these instructions to install and configure Microsoft Windows Server 2008 on new Application Servers.

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.

Important!

If using RAID, configure it before installing Windows Server 2008. Use a hardware RAID configuration only, and not a software RAID configuration. Set up the hardware RAID configuration as described in the vendor's documentation.

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.

Setting the primary DNS suffix

(Topic number: 7621)

Note:

This topic applies to Windows Server 2003 and Windows Server 2008.

When referring to the server running the IMPAX Business Services, 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

1. On Windows Server 2003, right-click **My Computer** and select **Properties**.

   or

   On Windows Server 2008, right-click **Computer** and select **Properties**.
2. If the operating system is Windows 2003, skip this step. On Windows Server 2008, click **Advanced System 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.
9. Log into Windows as an administrator-level user.

Installing IIS 7.0 in Windows Server 2008

(Topic number: 96439)

When installed on Windows Server 2008, IMPAX 6.5.1 requires IIS 7.0. IIS 7.0 can be installed through the Windows Server 2008 Server Manager tool.

To install IIS 7.0 in Windows Server 2008

1. Open the Windows Administrative Tools.

2. Select **Server Manager**.
3. In the left pane, click **Roles**.
4. In the right pane, click **Add Roles**.
5. If the Before You Begin screen appears, click **Next**.
6. On the Select Server Roles screen, select the **Web Server (IIS)** checkbox.
7. At the prompt, click **Add Required Features**.

   The .NET Framework 3.5 is included in the installation as a prerequisite for IIS 7.0.

   The Web Server (IIS) checkbox is now selected.
8. To continue, click **Next**.
9. On the Web Server IIS screen, click **Next**.

   A list of all IIS 7.0 features that are available to be installed is displayed, with the default features preselected.
10. Accept the defaults by clicking **Next**.
11. To continue, click **Next**.
12. On the Confirm Installation Selections screen, click **Install**.
13. On the Installation Results screen, click **Close**.

To quickly verify that IIS 7.0 is installed, you can type **http://localhost** in the Internet Explorer address bar. If IIS is successfully installed, the default IIS Welcome page appears.

Configuring Windows Server 2008

(Topic number: 95230)

To configure Windows Server 2008, several tasks are involved.

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.

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.

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.

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, folders and drives.**.
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: 47571)

Having a temporary directory on the server can be useful for storing files in the short term.

To create a temporary directory

1. In Windows Explorer, select the **C:** drive.
2. Select **File** > **New** > **Folder**.
3. Rename the new folder as **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.

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.

Partitioning disks on the Application Server on Windows 2008

(Topic number: 119085)

Use this topic when partitioning disks on an Application Server running Windows 2008.

We recommend partitioning the disks on the Application Server as described in this procedure. For security and performance reasons, we recommend that the Web Services that are installed with the IMPAX Business Services be placed on a drive other than C.

Recommended partition sizes

We recommend that you create the following disk partitions

Partition	Name	Size
C:\		40 GB
E:	WebServices	5–10 GB
L:	Logs	Rest
R:	Recovery	20 GB

To partition disks on the Application Server on Windows 2008

1. From the **Start** menu, select **Server Manager**.
2. Expand **Storage** and select **Disk Management**.

   The Initialize Disk dialog may appear. If so, select the disk(s) to initialize, then select **MBR** (Master Boot Record). Click **OK**.
3. Right-click the unallocated disk you want to format and select **New Simple Volume**.
4. In the wizard, click **Next**.
5. Accept all the space and click **Next**.
6. From the Assign the following drive letter list, select a drive letter using the preceding table as a reference.
7. Click **Next**.
8. From the Assign the following drive letter list, select the drive using the preceding table for drive names and letters.
9. Click **Next**.
10. Select **Format this volume** with the following settings:
    - File System to **NTFS**.
    - Allocation unit size to **Default**.
    - Volume label according to the preceding table.

- Select the **Perform a quick format** checkbox.

11. Click **Next**.
12. Click **Finish**.

    The partition is formatted.
13. Exit Disk Management.

Adding roles and role services in Windows 2008

(Topic number: 104586)

When installing the Application Server on a machine running Windows 2008, configure the following roles and role services immediately after 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 if Web Server (IIS) role is not added

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.

To add roles and role services in Windows 2008 if the Web Server (IIS) role is already added

1. Open the Windows Administrative Tools and select **Server Manager**.
2. From the pane on the left, select **Roles**.
3. In the right pane, under Web Services (IIS), click **Add Role Services**.
4. In the Add Role Services dialog, select the I**P and Domain Restrictions**, **IIS 6 Management Compatibility**,**ASP.NET**, **.NET Extensibility**, and **Dynamic Content Compression** checkboxes.
5. Click **Next** and follow the wizard.
6. To finish the installation, click **Install**.

    The installation could take several minutes.

Configuring IIS logging

(Topic number: 116031)

On Windows 2003 and Windows 2008 Application 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.

Installing third-party components on the Application Server

(Topic number: 119394)

Install the following third-party components on the Application Server if applicable.

- PC Anywhere (if applicable)
- Oracle Client (if applicable)
- Anti-virus software
- Adobe Acrobat Reader

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.

Installing and configuring the Oracle 10g Client for Windows

(Topic number: 6790)

Before installing the Oracle 10g Client, log into the server as a local administrator, and ensure that the network and TCP/IP are properly installed and configured.

Install the Oracle 10g Client software when using the Oracle Database Server, either on Solaris (AS3000) or Windows (AS300), and before connecting to an IMPAX RIS. The Oracle Client software is available for Windows 32-bit systems. It is installed on dedicated Application Servers, dedicated Curators, and dedicated AS300 Network Gateways and Archive Servers.

Note:

If installing the Application Server on the same machine as the AS300 server software, you do not have to install the Oracle 10g Client. The Oracle Server installed as part of the AS300 install contains the Client components.

If an earlier version of Oracle Client is installed on the system, uninstall that version (refer to page 131). If you have uninstalled a previous version of the Client, prior to installing the Oracle 10g Client, follow these steps.

Important!

Before installing the Oracle Client, disable virus protection software.

To install and configure the Oracle 10g Client for Windows

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

   Cygwin is automatically installed before Oracle is.
3. At the `Install Oracle "client" or "server"?` prompt, type **client**.
4. At the `Hostname of the Oracle server [] ?` prompt, type the correct host name of the IMPAX Database Server.
5. At the `What machine is the repository host? [localhost]` prompt, if it is the localhost, press **Enter**. Otherwise, specify the appropriate IP address.

6. At the `Where is the software repository?` prompt, if installing from the DVD drive on F, press **Enter**. Otherwise, type the DVD drive or software repository directory.
7. At the `Where is the temporary work directory? [ C:\cygwin\temp] ?` prompt, click **Enter** to accept the default location. Otherwise, type the directory to use.

   A series of messages appears as Oracle is installed and configured.
8. After the `Oracle installation complete` message appears, restart the server.

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

Setting up a connection to the Oracle database

(Topic number: 46341)

The Oracle 10g Client (version 10.2.0.4) software installs the drivers and programs required to communicate with the Oracle Server. Ensure that the network and TCP/IP are properly installed and configured.

To set up a connection to the Oracle database

1. If the Net Configuration Assistant is not open, select **Start** > **All Programs** > **Oracle - ohome** > **Configuration and Migration Tools** > **Net Configuration Assistant**.
2. In the Oracle Net Configuration Assistant Welcome dialog, select **Local Net Service Name configuration** and click **Next**.
3. If the Naming Methods Configuration dialog appears, select **Local Naming**. Click **Next**.
4. In the Net Service Name Configuration screen, select **Add**. Click **Next**.
5. In the Service Name field, type **MVF**. Click **Next**.
6. From the list of protocols, select **TCP**. Click **Next**.
7. In the TCP/IP dialog, type the hostname of the Oracle server.
8. Accept the default port number (1521). Click **Next**.
9. Select **Yes, perform a test**. Click **Next**.

   The first time the test runs, you see an error message. Ignore the error.
10. Click **Change Login**.
11. In the Username field, type **mvf**, and type the password for the mvf user.
12. Click **OK**.

    The test is performed again. The connection should be successful.
13. Click **Next**.
14. In the Net Service Name field, ensure that **MVF.world** appears. Click **Next**.
15. If you do not want to add a net service name for RIS, select **No**. Click **Next**.

    or

    To add a net service name for RIS, at the prompt to configure another net service name, select **Yes**. Click **Next**. Then repeat all previous steps using a different service name (for example,

qprod), as well as a different host name, login, and net service name (for example QPROD.WORLD).

16. In the Net Service Name Configuration Complete dialog, click **Next**.
17. In the Naming Methods Configuration Complete dialog, click **Next**.
18. To close the Net Configuration Assistant dialog, click **Finish**.

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.

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**.

Installing IMPAX Business Services

3

Follow the instructions to install the IMPAX Business Services and related software on the Application Server.

IMPAX Business Services: Order of installation tasks

(Topic number: 11232)

You must install and configure the software in the order it is listed.

Order	Software component
1	*Installing the IMPAX documentation* (refer to page 145)
2	*Installing the IMPAX Business Services* (refer to page 49)
3	*Configuring IIS error messages on Windows Server 2008* (refer to page 52)
4	*Verifying the Business Services installation* (refer to page 51)
5	*Installing multiple Application Servers and load balancing* (refer to page 49)
6	*Configuring the IMPAX Business Services* (refer to page 52)

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 128). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 143).

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* (refer to page 88)

Enabling active content for the Knowledge Base

(Topic number: 7700)

In Internet Explorer 7, all scripts on web pages are blocked by default. The IMPAX Knowledge Bases use JavaScript for their Search functionality and to render glossary definition popups. If JavaScript is blocked by the browser, when you view a Knowledge Base page, the definitions of the glossary terms rendered with JavaScript cannot be viewed, and searching is impossible. Therefore, enable active content.

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.

Enabling remote access to Knowledge Bases

(Topic number: 10019)

Perform this task to access Knowledge Bases installed on a different server (such as the Application Server).

To enable remote access to Knowledge Bases

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the Internet Options dialog, switch to the **Security** tab.
3. Select **Trusted sites**.
4. Click **Sites**.
5. In the Trusted sites dialog, if you are connecting to the Knowledge Base using http:// rather than https://, clear the **Require server verification (https:) for all sites in this zone** checkbox.

   We recommend that https:// be used.

6. In the Add this website to the zone field, type or paste the name of the Application Server that the Knowledge Bases are installed on (**https://*server_name***).
7. Click **Add**.
8. Click **Close**.
9. Click **Custom Level**. In the Security Settings dialog, under Scripting, ensure that **Active scripting** is enabled. Click **OK**.
10. Click **OK**.

Installing multiple Application Servers and load balancing

(Topic number: 11221)

For information on installing multiple Application Servers, refer to *Installing Application Servers in a load-balanced environment* (refer to page 156).

Installing the IMPAX Business Services

(Topic number: 9873)

The IMPAX Business Services must be installed.

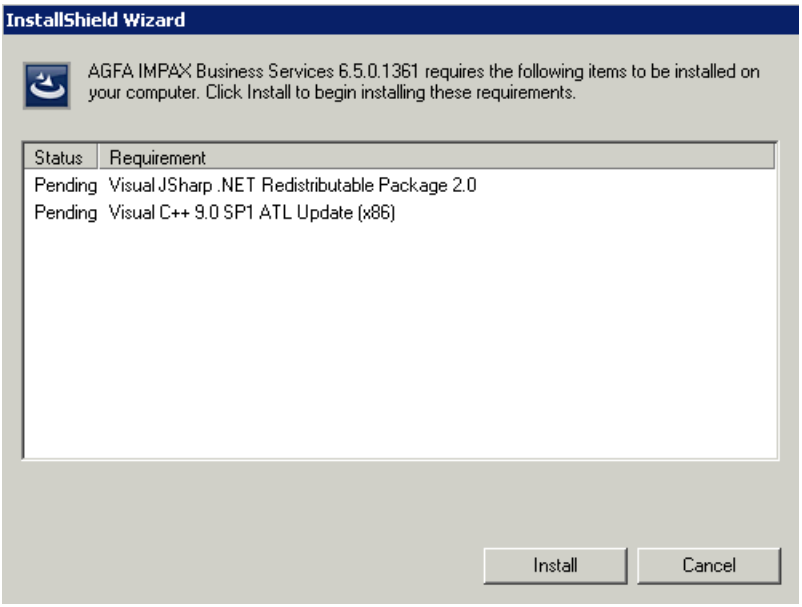
To install the IMPAX Business Services

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 on the Application Server prior to the upgrade.

   - 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.

   Note:

   We recommend installing the Web Services to E:\wwwroot for enhanced security. The installation folder name must not contain any special characters.

10. Click **Next**.
11. On the Setup Type screen, click **Custom**. Click **Next**.
12. If you have an IMPAX RIS to connect to, under RIS Web Services, select **This feature will be installed on local hard drive**. Click **Next**.

    By default, this option is not selected. Details on completing the connection to the RIS are available in "RIS configurations" (topic number 11329) in the *IMPAX 6.5.1 Application Server Knowledge Base*.

13. **Note:**

    This step is for NHS customers only.

If you want to enable NHS Smart Card authentication, where users can log into the computer and into IMPAX at the same time using a smart card, select **NHS Smart Card Web Services**. Click **Next**.

14. Click **Install**.

    The IMPAX Business Services are installed.

15. To continue with the configuration after the installation is complete and verified, select the **Launch Configuration tool** checkbox.
16. Click **Finish**.

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

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.

Configuring IIS error messages on Windows Server 2003

(Topic number: 7725)

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 2003

1. Open the Windows Administrative Tools and select **Internet Information Services (IIS) Manager**.
2. Expand ***computer_name*** > **Web Sites** > **Default Web Site**.
3. Right-click the **Documents** file and select **Properties**.
4. Switch to the **Custom Errors** tab.
5. In the list of Error messages for HTTP errors, select **404**.
6. Click **Edit**.

7. Under Message Type, select **URL**.
8. In the URL field, type **/AgfaHC.LanguageRedirect/LanguageRedirect.aspx**.
9. To close the two dialogs, click **OK** in each.
10. To close the Internet Information Services (IIS) Manager window, select **File** > **Exit**.

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**.

Configuring the IMPAX Business Services

(Topic number: 11246)

After the installation is complete, use the IMPAX Business Services Configuration Tool to configure the Application Server. Details on configuration are available in *Configuring the Application Server* (refer to page 53) and the *IMPAX 6.5.1 Application Server Knowledge Base*.

Configuring the Application Server

4

The following information provides content and information for configuring the Application Server to communicate with any IMPAX Client or Server.

Order of Application Server configuration

(Topic number: 11273)

You must configure the software in the order it is listed. For more information on installing the IMPAX software, consult *Installing the IMPAX Business Services (refer to page 49)*.

CAUTION!

If the site might install a load balancer in the cluster, follow the instructions in *Installing Application Servers in a load-balanced environment* (refer to page 156) before continuing.

1. *Generating the AS300 portable password file* (refer to page 54)
2. *Importing the portable password file* (refer to page 55)
3. *Connecting to the Agfa IMPAX database* (refer to page 56)
4. *Extending the database schema* (refer to page 59)
5. *Armoring the Application Server* (refer to page 59)
6. *Adding the LDAP IP address to the Application Server's hosts file on Windows Server 2003* (refer to page 60)
7. *Adding the LDAP IP address to the Application Server's hosts file on Windows Server 2008* (refer to page 61)
8. *Creating an SSL certificate request* (refer to page 62)
9. *Submitting a certificate request to a certificate authority* (refer to page 63)

10. *Importing an SSL certificate in the Security Wizard* (refer to page 64)
11. *Creating the administration account* (refer to page 65)
12. *Connecting to the ADAM/AD LDS server* (refer to page 66)
13. *Compressing web services communication on the Application Server* (refer to page 68)
14. *Configuring the image upload server* (refer to page 68)
15. *Connecting IMPAX Application Server to Audit Manager* (refer to page 69)
16. *Enabling and disabling the audit fallback log* (refer to page 69)
17. *Setting the logging levels* (refer to page 70)
18. *Configuring the connection to a RIS* (refer to page 70)
19. *Synchronizing clocks on Windows-based IMPAX systems* (refer to page 75)
20. *Completing the IMPAX Server configuration* (refer to page 78)

Generating the AS300 portable password file

(Topic number: 7694)

To install the other components, you must generate a password file from the Database Server to synchronize passwords between the components. The file contains all of the user IDs and passwords for all default IMPAX users. The file must be copied to other components as requested during those installations.

To generate the AS300 portable password file

1. On the Database Server, open a command prompt.
2. Change to the **C:\mvf\bin** directory.
3. Type

   passkey -M EXPORT -k *temporary_password*

   where *temporary_password* is the password used to import the password file when installing or configuring the other components.

The password file is created in C:\mvf\mvf.portable.psd.

CAUTION!

The mvf.portable.psd file contains sensitive information. To ensure that the security of the system is maintained, delete the password file after all required components are installed.

Generating the AS3000 portable password file

(Topic number: 58083)

You may need to generate the portable password file to install new servers or to troubleshoot when password file import fails during installation.

To generate the AS3000 portable password file

1. Log into the AS3000 Database Server machine as the **root** user.
2. Change to the **/usr/mvf** directory.
3. To export the passkey for installing IMPAX on remote machines, type

   ./bin/passkey -M EXPORT -k *temporary_password*

   where *temporary_password* is a password to be used to import the portable password file later.

   This creates the /usr/mvf/mvf.portable.psd password file.
4. On the target server, open a Cygwin command window to download the portable password file from the Database Server.
   a. Ensure the C:\temp directory exists on the target server. If the C:\temp directory does not exist, create one.
   b. Double-click the Cygwin.bat file located in the C:\cygwin\ directory.
   c. On the Cygwin command window, type

      scp service@<Database server hostname>:/usr/mvf/mvf.portable.psd /cygdrive/c/temp
   d. If prompted to add the Database Server's RSA key fingerprint to the list of known hosts, click **Yes**.

      The portable password file is downloaded to the C:\temp directory on the target server.

      Important!

      You should know the service user's password on the Database Server before downloading the portable password file.

Delete /usr/mvf/mvf.portable.psd from the Database Server when you are finished downloading it to the target servers or servers.

Importing the portable password file

(Topic number: 7687)

Import the generated portable password file so that the IMPAX Business Services can successfully connect to the database server software.

To import the portable password file

1. To open the Business Services Configuration Tool, select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Configuration Tool**.
2. Switch to the **Security** tab.
3. Click **Import Password**.
4. Navigate to the mvf.portable.psd file and click **Open**.
5. At the prompt, enter the same *temporary_password* used when generating the portable password file (refer to page 54).
6. Click **OK**.
7. At the confirmation message, click **OK**.

Connecting to the Agfa IMPAX database

(Topic number: 11303)

Follow the procedure applicable to the type of IMPAX database installed: an Oracle database or a SQL Server database.

Creating an Oracle ODBC data source

(Topic number: 59290)

If your IMPAX cluster has an Oracle database, configure the Application Server to communicate with the Oracle database that contains the patient information.

Note:

You must have the Oracle 10g Client installed before configuring the connection. For installation instructions, refer to *Installing and configuring the Oracle 10g Client for Windows* (refer to page 132).

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

To complete the connection, perform this procedure: *Connecting the Business Services to an Oracle database* (refer to page 57).

Connecting the Business Services to an Oracle database

(Topic number: 11355)

If your IMPAX cluster has an Oracle database, configure the Application Server to communicate with the Oracle database that contains all the patient information.

Note:

Before performing this task, you should have completed the following: *Creating an Oracle ODBC data source* (refer to page 56).

To connect the Business Services to an Oracle database

1. Open the 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.

Connecting the Business Services to the SQL Server database

(Topic number: 7713)

If your IMPAX cluster has an SQL Server database, configure the Application Server to communicate with the SQL database that contains all the patient information.

To connect the Business Services to the SQL Server database

1. Open the Business Services Configuration Tool.
2. Switch to the **Database** tab.
3. Under PACS Database Settings, select **SQL Server**.
4. In the SQL Server Name field, type the SQL Server database server name.
5. Click **Configure ODBC**.
6. In the ODBC Data Source Administrator dialog, switch to the **System DSN** tab.
7. Click **Add**.
8. In the Create New Data Source dialog, select **SQL Server**. Click **Finish**.
9. In the Create a New Data Source to SQL Server dialog, as the Name, type **mvf_sql**.
10. As the Description, type **mvf**.
11. From the Server list, select the name of the SQL Server. Click **Next**.
12. Click **SQL Server Authentication**.
13. Ensure that the **Connect to SQL Server to obtain** checkbox is selected.
14. As the Login ID, type **mvf**.
15. As the Password, type **mvf**.
16. Click **Client Configuration**.
17. In the Add Network Library Configuration dialog, ensure that **TCP/IP** is selected. Click **OK**.
18. Click **Next**.
19. Select the **Change the default database to** checkbox.
20. From the list, ensure that **mvf** is selected. Click **Next**.
21. Clear the **Perform translation for character data** checkbox. Click **Finish**.
22. To test the connection, click **Test Data Source**.
23. When prompted that the connection was successful, click **OK**.
24. To close the ODBC Microsoft SQL Server Setup dialog, click **OK**.
25. To close the ODBC Data Source Administrator dialog, click **OK**.
26. In the IMPAX Business Services Configuration tool, click **Test**.
27. If the message `Connection to SQL Server database successful` appears, click **OK**.

    If the test fails, verify that the SQL 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. Open the Business Services Configuration Tool.
2. Switch to the **Database** tab.
3. Ensure that your SQL (refer to page 58) or Oracle (refer to page 57) 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 the Application Server.
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.

Adding the LDAP IP address to the Application Server's hosts file on Windows Server 2003

(Topic number: 119697)

To redirect traffic to the LDAP server, add the LDAP server's IP address to the Application Server's hosts file.

To add the LDAP IP address to the Application Server's hosts file

1. On the Application Server, navigate to the \windows\system32\drivers\etc directory.
2. Open the **hosts** file.
3. Add the LDAP server's IP address to the hosts file. In the following example, the LDAP server's IP address is the last line of the hosts file.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
```

```
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
102.97.56.103   ldapserver.agfa.com    #The LDAP server
```

4. Save the hosts file.

Adding the LDAP IP address to the Application Server's hosts file on Windows Server 2008

(Topic number: 130299)

To redirect traffic to the LDAP server, add the LDAP server's IP address to the Application Server's hosts file.

To add the LDAP IP address to the Application Server's hosts file

1. On the Application Server, navigate to the \windows\system32\drivers\etc directory.
2. Open the **hosts** file.
3. Add the LDAP server's IP address to the hosts file. In the following example, the LDAP server's IP address is the last line of the hosts file.

```
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
::1             localhost
102.97.56.103   ldapserver.agfa.com    #The LDAP server
```

4. Save the hosts file.

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.

Opening the Security Wizard

(Topic number: 11429)

Open the Security Wizard to manage your SSL certificates and the default security settings.

To open the Security Wizard

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.

The Security Wizard is displayed.

Creating an SSL certificate request

(Topic number: 7709)

Generate a certificate request that can be submitted to a trusted certificate authority (refer to page 63). 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 64).

Note:

In a single IMPAX cluster environment, you create one certificate for the Application Server. In a load balanced environment, you create one certificate for each application server for access to ADAM/AD LDS services. Then you create one certificate with the settings of the load balancer for communicating through IIS, which you subsequently copy to each Application Server.

To create an SSL certificate request

1. Open the Security Wizard (refer to page 62).
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.

   CAUTION!

   Selecting **Copy the information to the clipboard** may introduce a security risk, as all information about the IMPAX Application Server and its network settings is included in the certificate request.

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 62).

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 64).

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 (refer to page 62).

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 (refer to page 62).
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 Application Server.

To create the administration account

1. Open the IMPAX Business Services Configuration Tool.
2. Switch to the **Security** tab.
3. Click **Security Wizard**.

4. On the Agfa Security Wizard screen, select **Work with the Application Server default settings**. Click **Next**.
5. On the Web Services URL Configuration screen, click **Next**.
6. 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**.
7. Click **Add Administration License**.
8. 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.
9. Select the administration license and click **Open**.
10. Click **Finish**.
11. 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 ADAM/AD LDS server

(Topic number: 11135)

The ADAM server is a database that maintains all the security around user profiles, access controls, and station information on systems running Windows Server 2003. The AD LDS server performs the same function on systems running Windows Server 2008. Connect to the ADAM/AD LDS server so that IMPAX Client users can be added.

Note:

When the primary instance of ADAM/AD LDS is on the Application Server you are configuring, the fully qualified domain name and port number are automatically populated from the DSN information on the computer. If you are connecting to an ADAM/AD LDS instance on another Application Server, the domain and hostname must point to that server.

To connect to the ADAM/AD LDS server

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

3. In the Server Fully Qualified Hostname field, enter the domain and host name of the ADAM/AD LDS server.

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

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

   The default port number of the ADAM/AD LDS server is 636.

5. Click **Apply**.

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.

Note:

When the primary instance of AD LDS is on the Application Server you are configuring, the fully qualified domain name and port number are automatically populated from the DSN information on the computer. If you are connecting to an AD LDS instance on another Application Server, the domain and hostname must point to that server.

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.

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

   The default port number of the AD LDS server is 636.

5. Click **Apply**.

Compressing web services communication on the Application Server

(Topic number: 11406)

Compressing web services communication may increase communication flow performance between the IMPAX Clients and the Application Server over slow networks such as VPNs or slow WANs. Compression reduces the size of the communication messages, making them transfer more quickly between systems. The message transfer speeds may vary depending on the computer running the Client. This is a performance trade-off, since the Client and Application Server consume additional CPU time due to compression and decompression, which increases message delivery latency.

Note:

We recommend disabling compression for containers with Clients on high-speed gigabit networks.

On the Application Server, compression is always turned on by default. This configuration option can be accessed through the Configure area - Station section of the Client. For additional information on setting compression in the Client, refer to "Compressing web services communication on the Client for improved performance" (topic number 9390) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Configuring the image upload server

(Topic number: 11402)

Imported images or CDs are uploaded to an image server, which can include the Archive Server, Database Server, web caches, and image caches. Typically this server is configured using the Image Access Manager. Using this manager, you can specify one or more Application Servers as image sources. Available image servers (as destinations) are grouped by priority—among available online servers, higher-priority destinations are preferred to lower-priority destinations.

To configure the image upload server

1. To configure the required SCP, use the Image Access Manager in the Administration Tools.

   Refer to "Modifying image distribution responsibilities for a source station" (topic number 32193) in the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*.

Note:

If the Image Access Manager configuration is not accurate for your site, you can modify the SCP AE title value in the AgfaHC.Pacs.Web/web.config file by providing a value in the ScpAETitle field. If this value is provided, all images are uploaded to the indicated image server, bypassing the Image Access Manager configuration.

Connecting IMPAX Application Server to Audit Manager

(Topic number: 11444)

By establishing a connection to an audit server, such as Audit Manager 1.2, you can keep a record of the events accessing protected health information that occur on the Clients and servers. This record can identify when changes were made, what the changes were, and who made the changes.

To connect IMPAX Application Server to Audit Manager

1. Open the Business Services Configuration Tool.
2. Switch to the **Windows Services** tab.
3. Under Protected Health Information Disclosure Auditing, in the hostname field, type the IP address of the Audit Manager.
4. Verify that the port number is set to **514**.
5. In the Max Message Size field, type the maximum size of an audit message in bytes.
6. Restart the IMPAX Audit Event Log Manager service in the services.msc.
7. Log into Audit Manager.
8. In the navigator, open the **Administration** menu.
9. Click **Dynamic Settings**.
10. In the Allowed Client IP addresses list, enter appropriate IP addresses or remove all to accept messages from all.
11. Click **Save**.

Enabling and disabling the audit fallback log

(Topic number: 11441)

The audit fallback log is a local log file that contains the information sent to the audit server. The location for this log file is C:\Program Files\Agfa\Sec\Audit\log.

To enable or disable the audit fallback log

1. Open the Business Services Configuration Tool.
2. Switch to the **Windows Services** tab.
3. Under Protected Health Information Disclosure Auditing, to start saving a local copy of the audit log, select the **Enable Fallback Log** checkbox.

   or

   To stop saving a local copy of the audit log, clear the **Enable Fallback Log** checkbox.

4. Click **Apply**.

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.

Configuring the connection to a RIS

(Topic number: 11313)

By identifying the RIS Database Server, the IMPAX Client can include additional patient, study, order, and report information in the Text Area.

Order	Task
1	Prepare the Application Server for connection to an IMPAX RIS (refer to page 71).
2	Configuring the connection to the IMPAX RIS database (refer to page 73)
3	Connect the Application Server to a (non-IMPAX) RIS (refer to page 74).

Preparing the Application Server for connection to an IMPAX RIS

(Topic number: 11347)

To prepare the Application Server for connecting to an IMPAX RIS, perform these initial setup tasks. By identifying the IMPAX RIS database server on the Application Server, the IMPAX Client can include additional patient, study, order, and report information in the Text area. For additional information on the IMPAX Client Text area, refer to "Text area overview" (topic number 8124) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Note:

If the site does not have an IMPAX RIS to connect to, refer to Connecting the Application Server to a non-queryable RIS or Connecting the Application Server to a queryable RIS (refer to page 74) instead.

To prepare the Application Server for connection to an IMPAX RIS

1. Ensure the Oracle 10g Client is installed.

   For instructions on how to install the Oracle 10g Client, refer to Installing and configuring the Oracle 10g Client for Windows (refer to page 132).

2. Install the RIS services on the Application Server.

   For instructions on how to install RIS services, see *Installing the RIS services on the Application Server* (refer to page 71).

3. Change the paths to the IMPAX RIS for StudyInfoService, OrderInfoService, and PatientInfoService.

   For instructions on how to change these paths, see *Changing the RIS web services paths* (refer to page 72).

4. Configure the connection between the Oracle 10g client and the IMPAX RIS.

   For instructions on how to configure this connection, see Configure the connection between the Oracle 10g client and the IMPAX RIS (refer to page 73).

Installing the RIS services on the Application Server

(Topic number: 49120)

To ensure the correct services are available during configuration, install the RIS web services on the Application Server.

Note:

Complete this task on all Application Servers in the cluster.

To install the RIS services on the Application Server

1. On the Application Server computer, insert the IMPAX Business Services CD.

2. Browse to the **appserver** folder containing the Business Services software.
3. Run **agfa impax business services setup.exe**.
4. In the Welcome screen, click **Next**.
5. Select **I accept the terms in the license agreement**. Click **Next**.
6. Select **Custom**. Click **Next**.
7. Under **RIS Services**, select **AgfaHC.Ris.Web.Service**. Click **Next**.
8. Click **Install**.

   The RIS web services are installed.
9. When asked if the computer can be restarted, click **Yes**.
10. When the computer restarts, the Installation dialog is displayed. Click **Finish**.

Changing the RIS web services paths

(Topic number: 49123)

Modify the paths in the StudyInfoService, OrderInfoService, and PatientInfoService to remove the default references to the IMPAX database.

Note:

Complete this task on all Application Servers in the cluster.

To change the RIS web services paths

1. Start the IMPAX Client and log in.
2. From the **Configure** drawer menu, select **Stations**.

   You must have the correct license and permissions to perform this task.
3. In the navigation pane, select a station container.

   You can only edit access to business services for station containers; therefore, ensure that you have organized your stations to match how you want the access defined. For details, refer to "Determining how stations should be organized" (topic number 9359) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.
4. In the details pane, expand the **General** bar.
5. Switch to the **Services Access** tab.
6. In the table, locate the **StudyInfoService**.
7. Change the path from **/AgfaHC.Pacs.Web.Services/MvfStudyInfoWebService.asmx** to **/AgfaHC.Pacs.Web.Services/StudyInfoWebService.asmx** so the *Mvf* reference is removed from the path.
8. Repeat steps 6 and 7 for the **OrderInfoService** and **PatientInfoService**.

   The changes are saved automatically when you switch context.
9. To make the changes take effect, restart all IMPAX Client stations.

Configuring the connection to the IMPAX RIS database

(Topic number: 109618)

You must configure the IMPAX Application Server to connect to the IMPAX RIS database.

To configure the connection to the IMPAX RIS database

1. On the Application Server, open the IMPAX Business Services Configuration Tool. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Configuration Tool**.
2. Switch to the **Database** tab.
3. Under RIS Database Settings, type the Service Name (DBNAME) as configured in the TNSNAMES.ORA file. Information on how to set up the TNSNAMES.ORA file using Net Configuration Assistant can be found in *Setting up a connection to the Oracle database* (refer to page 133).

Connecting the Oracle 10g Client to the IMPAX RIS database

(Topic number: 49126)

To retrieve reports and display them in the IMPAX Client Text area, establish a connection between the Oracle 10g Client and the IMPAX RIS database.

Note:

You must have the Oracle 10g Client installed before configuring the connection. For installation instructions, refer to "*Installing and configuring the Oracle 10g Client for Windows* (refer to page 132)" in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

To connect the Oracle 10g Client to the IMPAX RIS database

1. Select **Start** > **All Programs** > **Oracle - ohome** > **Enterprise Manager Console**.
2. Under Network, right-click the **Database** folder and select **Add Database to Tree**.
3. In the Add Database to Tree dialog, in the **Hostname** field, type the name of the IMPAX RIS database.
4. In the **Port** field, accept the default value of **1521**.
5. In the **SID** field, type **QDOC**.
6. In the Net Service Name field, type ***RIS_Service_Name***.

   where *RIS_Service_Name* is the service name of the IMPAX RIS database.
7. Click **OK**.
8. Close the Enterprise Manager Console.

Connecting the Application Server to a queryable RIS through the Connectivity Manager

(Topic number: 11346)

The Connectivity Manager is a middleware component in the integration between HIS, RIS, modalities, and PACS systems, linking patient and study data with images. To display report information available from a queryable RIS in the Text area of IMPAX, connect to the Connectivity Manager. For additional information on the IMPAX Client Text area, refer to "Text area overview" (topic number 8124) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

To connect the Application Server to a queryable RIS through the Connectivity Manager

1. Open the Business Services Configuration Tool.
2. Switch to the **Web Services** tab.
3. In the Report Info Sources area, click **Add**.
4. In the Edit Report Source dialog, in the **Report Source Provider** field, type the Default Assigning Authority name identified when the Connectivity Manager custom RIS mappings were configured.

   A maximum of 16 characters can be entered in this field.
5. From the **RIS Type** list, select **Connectivity Manager Queryable RIS**.
6. In the **URL** field, type the following:

   http://*Connectivity_Manager_Server*/CMReportServerInterface/CMReportServer.asmx
7. To close the Edit Report Source dialog, click **OK**.
8. To close the Business Services Configuration Tool, click **OK**.

Configuring the Application Server to check for a RIS report dictation license

(Topic number: 120724)

Note:

Perform this task only when using RIS embedded reporting with embedded Nuance SpeechMagic support.

When a user attempts to dictate a report on the IMPAX Client using embedded RIS reporting with integrated speech recognition, the Application Server checks that there is a valid QDictate license on the configured FlexLM license server. If no license is available, reports cannot be dictated.

To configure the Application Server to check for a RIS report dictation license

1. From the **Start** menu, select **All Programs** > **Agfa Healthcare** > **Business Services** > **Configuration Tool**.
2. In the Agfa IMPAX Business Services Configuration dialog, switch to the **RIS** tab.

3. Under RIS License Settings, in the FlexLM License Server field, type the address of the FlexLM server you want the Application Server to check for the QDictate license (or the local path if the license is copied locally).

   For example, type

   27000@192.168.1.149 or **C:\licenses\QDictate.lic**

4. Click **Apply**.
5. Click **OK**.

The value you type in the FlexLM License Server field is stored in the Windows registry. The Application Server uses this value to determine which FLexLM license server should be checked for the QDictate license.

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

Completing the IMPAX Server configuration

(Topic number: 11320)

Now that the Application Server is installed, complete the configuration of IMPAX Server software. For information on configuring disk backups and performing the initial system configuration in the Administration Tools, refer to your Server configuration guide.

Managing IMPAX licenses

5

The following information provides content and information for installing licenses on the Application Server using the License Manager.

Administering IMPAX licenses with the Service Portal

(Topic number: 107303)

Use the Agfa Web Service Portal (Service Portal) to view, install, assign, cancel, and uninstall IMPAX Client licenses.

Logging into the Service Portal

(Topic number: 106846)

The Service Portal is a web-based tool used to support, maintain, and monitor the IMPAX system. If the Service Portal is configured to use secure sockets (SSL), the machine running the browser must have the correct SSL certificate installed.

Use a web browser to log into the Service Portal. The recommended browser is Internet Explorer 7.0 or higher.

Note:

You must be logged into IMPAX as an administrator to access the Service Portal.

To log into the Service Portal

1. Open a web browser.

2. In the address field, type **http://*application_server*/portal/**

   where *application_server* is the IP address or full qualified domain name of the Application Server where the Service Portal is installed.

3. Type the IMPAX administrator user name and password.

   The password is case-sensitive. If you cannot log in, check whether Caps Lock is enabled on your keyboard.

4. From the Domain list, select the domain to log into.
5. Click **Log-in**.

From the Service Portal's home page, you can monitor the health of the IMPAX system, and view, install, activate, and manage licenses.

Installing and activating a Client license with the Service Portal

(Topic number: 106848)

To run the IMPAX Client software, you must install and activate relevant licenses on the Application Server. Use the Service Portal to install and activate Client licenses.

Note:

If you attempt to install and activate a license before or after the dates specified by the license's Date Range field, the license is installed but not activated.

To install and activate a Client license with the Service Portal

1. Log into the Service Portal (refer to page 79).
2. From the menu on the left-hand side of the Service Portal's main page, expand **Home** and **License Management**, if necessary.
3. Click **Install License**.
4. Click **Browse**.
5. In the Choose File dialog, navigate to the folder where the license file you want to install is located.
6. Select the license file and click **Open**.
7. Click **Install and Activate License**.

   Note:

   If the current date is not within the date range specified by the license's Date Range field, the license is installed but not activated.

   If the license is installed and activated, a confirmation message is displayed. If the license has already been activated, an error message is displayed.

Activating an installed but inactive license using Service Portal

(Topic number: 107093)

When using the Service Portal to install a license, the license can be installed and activated at the same time. However, you may find that some licenses have been installed without being activated. This situation can arise if you attempt to install and activate a license before or after the dates specified in the license's Date Range or when the hardware key validation fails.

To activate an inactive license, first check that the current date falls within the range of dates specified in the Date Range field of the license you are attempting to activate. If the current date is before or after the specified dates, you cannot activate the license.

To activate an installed but inactive license using Service Portal

1. Log into the Service Portal (refer to page 79).
2. From the menu on the left-hand side of the Service Portal's main page, expand **Home** and **License Management**, if necessary.
3. Click **Manage Licenses**.

   All installed licenses are displayed in the Licenses Information table (refer to page 82). A black dot beside a license indicates that the license is installed but not activated.
4. In the Serial Number column of the license you want to activate, click the link.

   The license details are displayed in the **License Information** text box. As the license is inactive, no active users are displayed below the **License Information** text box.
5. To activate the license, click **Activate License**.

Viewing license information in the Service Portal

(Topic number: 123812)

View license information in the Service Portal to see the types of licenses installed on the system, the number of active users for a license, if a license has expired, and so on.

To view license information in the Service Portal

1. Log into the Service Portal (refer to page 79).
2. From the menu on the left-hand side of the Service Portal's main page, expand **Home** and **License Management**, if necessary.
3. Click **Manage Licenses**.

   All installed licenses are displayed in the Licenses Information table (refer to page 82). Licenses highlighted red are in the grace period or have expired.
4. To view additional information about a specific license, in the Serial Number column of the license, click the link.

The license details are displayed. If the license is in use, a list of active users is displayed in the Active Users table. The users and host machines that have reserved the license are listed in the Reservation Information column.

5. To refresh the list of active users for a specific license, click **Refresh**.

Service Portal license information: Available columns

(Topic number: 123797)

When viewing license information in the Service Portal, you are presented with the following information:

Column	Description
Active	Shows the status of the license: active (green) or inactive (black).
Serial Number	Displays the serial number of the license. Click the link to view additional details for a specific license.
License Name	Shows the name of the license such as Radiologists with QC, Administrator, and so on.
Admin Name	Displays the name of the administrator for the license.
Type	Displays the type of license; for example, demo, ADMIN, RAD, BRSTIM, and so on.
Install Date	Provides the date when the license was installed on the system.
Grace Period End Date	Provides the date when the grace period for the license ends. The grace period (if applicable to the license) is the amount of time after the license expires that IMPAX can continue to be used.
Total	Lists the total number of licenses available. *Site* indicates that an unlimited number of licenses are available for use at the site.
Available	Lists how many licenses are available for use. *License* indicates that an unlimited number of licenses are available for use at the site.

Canceling a license reservation for a specific workstation

(Topic number: 107262)

You can cancel a license reservation for a user who is logged in and consuming a license. After approximately 30 minutes, the Client must request a license from the Application Server. If the request is denied, the Client is logged off.

To cancel a license reservation for a specific workstation

1. Log into the Service Portal (refer to page 79).
2. From the menu on the left-hand side of the Service Portal's main page, expand **Home** and **License Management**, if necessary.

3. Click **Manage Licenses**.

   All installed licenses are displayed in tabular format. A green dot in the Active column indicates that the license has been activated. License reservations can be made for activated licenses only.

4. In the Serial Number column of the license which you want to cancel a reservation for, click the link.

   The license details are displayed. If the license is in use, a list of active users is displayed in the Active Users table. The users and host machines that have reserved the license are listed in the Reservation Information column.

5. From the table, identify the user and host machine whose license reservation you want to cancel and click **Cancel**.

   The Client will request a new license after about 30 minutes. As the license has been cancelled, the renew request fails and the Client is logged off.

Uninstalling a license using the Service Portal

(Topic number: 107123)

You can uninstall a license using the Service Portal.

Note:

If you uninstall a license with active users, those Clients must wait for 30 minutes before requesting another license from the Application Server. If the request is not granted, the Client is logged off.

To uninstall a license using the Service Portal

1. Log into the Service Portal (refer to page 79).
2. From the menu on the left-hand side of the Service Portal's main page, expand **Home** and **License Management**, if necessary.
3. Click **Manage Licenses**.

   All installed licenses are displayed in tabular format. A green dot in the Active column indicates that the license has been activated. A black dot indicates that the license is installed but not activated. You can uninstall any license listed, whether activated or not.

4. In the Serial Number column of the license you want to uninstall, click the link.

   The license details are displayed. If the license is in use, a list of active users is displayed below the license information.

5. Click **Uninstall License**.
6. At the uninstall confirmation prompt, click **OK**.

   The license is uninstalled. If there are any active users of the license, these Clients must request a new license after approximately 30 minutes.

Administering licenses with the License Manager

(Topic number: 49395)

The License Manager is a tool for viewing, installing, assigning, cancelling, and uninstalling licenses.

Opening the License Manager Administrator Tool

(Topic number: 11398)

Open the License Manager Administrator Tool to manage your licenses. Use the License Manager Administrator Tool to install and activate new licenses on the Application Server.

Important!

You must have the Administrator license installed on the Application Server before opening the Licence Manager Administrator Tool.

To open the License Manager Administrator Tool

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

Installing a license using License Manager

(Topic number: 11390)

When a license is received at the site, it must be installed and activated on the Application Server before it can be used by the IMPAX Clients.

To install a license using License Manager

1. Open the License Manager Administrator Tool (refer to page 84).
2. Ensure 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. Activate the license (refer to page 85).

   Once activated, the licenses can be used by the IMPAX Clients.

Renaming a license using License Manager

(Topic number: 11394)

Licenses have generic names that do not clearly identify their purpose. Use the setAdminName command to give the license 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 Entry Level Radiologist.

To rename a license using License Manager

1. Open the License Manager Administrator Tool (refer to page 84).
2. Ensure you are at the **C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool** prompt.
3. At the prompt, type the following:

   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"**.

Activating a license using License Manager

(Topic number: 11395)

A license that has been installed on the Application Server must be activated before it can be used by the IMPAX Clients at the site.

To activate a license using License Manager

1. Open the License Manager Administrator Tool (refer to page 84).
2. Ensure you are at the **C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool** prompt.
3. 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.

For additional information, refer to "Managing licenses" (topic number 9351) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

To make the license accessible, assign the license to a role.

Uninstalling a license using License Manager

(Topic number: 11383)

If a license becomes obsolete or is no longer valid, you must remove it from the Application Server. An obsolete or invalid license cannot be associated with a role.

To uninstall a license using License Manager

1. Open the License Manager Administrator Tool (refer to page 84).
2. Ensure you are at the **C:\Program Files\Agfa\Impax Business Services\Licensing Admin Tool** prompt.
3. At the prompt, type the following:

   almadmin -unInstall *serialnumber-revisionNumber*

   where *serialnumber-revisionNumber* is the serial number of the license to be uninstalled. For example, type **almadmin -unInstall 0001234567-2**.

Completing optional configurations

6

The following information provides content and information for optional configurations for the Application Server.

Creating the Client login message

(Topic number: 11298)

Create a login message to appear on the IMPAX Client login screen. If the site is planning to configure IMPAX to use local Windows authentication, do not perform this step, as local Windows authentication does not display this login message.

Note:

In a cluster with multiple Application Servers, the login message must be the same between all Application Servers.

To create the Client login message

1. On the Application Servers, navigate to:

   <drive>:/wwwroot/AgfaHC.User.Security.Web.Services/

2. Open the **web.config** file.
3. Search for:

   ```
   <LoginMessage>Thank you for choosing Agfa HealthCare.</LoginMessage>
   ```

4. Change the "Thank you for choosing Agfa HealthCare" message as required.
5. Save and close the web.config file.

Changing the link to the IMPAX Client Installer web page

(Topic number: 11323)

The iisstart.html page contains a link to the IMPAX Client Installer. By default, this link is set to open the IMPAX Client Installer folder on the Application Server. If the IMPAX Client Installer is going to be installed on any other server, the path in the link must be changed to point to the correct server.

Note:

This task may also be completed after the IMPAX Client Installer has been installed.

To change the link to the IMPAX Client Installer web page

1. On the Application Server, using Notepad open **E:\inetpub\wwwroot\iisstart.htm**.
2. Search for **http://localhost/clientinstaller/**, and change **localhost** to the name of the server hosting the IMPAX Client installer package.
3. Save the changes to the iisstart.htm page.

   All users accessing the IMPAX Client Installer web page through the link on the iisstart.html page are now directed to the correct location.

Viewing translated documentation from the IMPAX Client Help menu

(Topic number: 131745)

The IMPAX Client Knowledge Base (available in English) is a comprehensive set of information that details how radiologists, clinicians, specialists, and PACS administrators configure and use the IMPAX Client software. The IMPAX Client Knowledge Base: Core is available in Bulgarian, Croatian, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Italian, Norwegian, Polish, Portuguese, Romanian, Russian, Simplified Chinese, Spanish, Swedish, and Traditional Chinese. As long as it is installed on the Application Server, the Knowledge Base is displayed in those languages based on the Windows Locale setting of the computer.

To view translated documentation from IMPAX Client Help menu

1. Install the documentation in the languages you need (e.g. English and French). Instructions on how to install the IMPAX 6.5.1 documentation are in the topic *Installing the IMPAX documentation* (refer to page 145)
2. Change the regional settings to the language you need (e.g. French).
3. Open the IMPAX Client.

4. Click **F1** or go to the Help menu and select **Getting started**.

   The selected page of the Knowledge Base is displayed in a browser window, in the IMPAX interface language you selected. If the Knowledge Base is not available in the interface language (usually because that Knowledge Base was not installed), you must manually redirect the URL to the English Knowledge Base each time you open a page.

Viewing East Asian characters in the IMPAX Client

(Topic number: 11257)

To display East Asian (Chinese, Japanese, Thai) characters correctly in the IMPAX Client study comments, Advanced Search, and what fields are available in the Client, modify the web.config file.

To view East Asian characters in the IMPAX Client

1. Navigate to **E:\inetpub\wwwroot\AgfaHC.Pacs.Web.Services**.
2. Open the **web.config** file.
3. Search for <**add key="UseMvfUtf8Fields"value="false"**> and change the value to **true**.

   CAUTION!

   Changing other key values can break system features.

4. Save and close the web.config file.
5. Clear the isolated storage.

   The files in isolated storage are refreshed based on the last updated date of the data in the database, which does not change when the useMvfUtf8Fields value is modified. The files in the isolated storage can be safely cleared and are sent to the Application Server when empty.

Improving image viewing speed

(Topic number: 11286)

If the site has configured a proxy server for accessing the internet, viewing images on an IMPAX Client is significantly slower. To improve the communication speed, turn off the Quality of Service setting.

To improve image viewing speed

1. Open Control Panel.
2. Double-click **Network Connections**.
3. Right-click the network connection and select **Properties**.
4. Clear the **QoS Packet Scheduler** checkbox.

5. Click **OK**.

Configuring IMPAX to use local Windows authentication

(Topic number: 11281)

By configuring the Application Server to use local Windows authentication, users can log into the computer and into IMPAX at the same time. This single-sign on option saves users the time involved in logging into IMPAX separately.

Note:

These instructions assume you have already installed the IMPAX Business Services.

To configure IMPAX to use local Windows Authentication

1. On the Application Server, navigate to E:*wwwroot*\WindowsAuthentication.
2. Open the **web.config** file in a text editor such as Notepad.
3. In the Notepad file, search the web.config file for the text:

   <**Plugin Name="mydomain"**
4. Modify the *mydomain* value with the friendly name of the domain. This can be any intuitive name.

   This must be the same domain name identified in the AgfaHC.User.Administration.Web.Services/web.config and AgfaHC.User.Security.Web.Services/web.config files.
5. Modify the default Path value so that it points to the correct location of the .dll files. On your local system, this location may be different from the default path.
6. Save and close the web.config file.

Adding the Application Server as a trusted site on the IMPAX Client

(Topic number: 11331)

Any IMPAX Client wanting to use integrated Windows authentication must list the Application Server as a trusted site.

To add the Application Server as a trusted site on the IMPAX Client

1. Launch Internet Explorer.
2. In Internet Explorer, select **Tools** > **Internet Options**.

3. In the Internet Options dialog, switch to the **Security** tab.
4. Select **Local Intranet**.
5. Click **Sites**.
6. Click **Advanced**.
7. In the Local Intranet dialog, locate the Application Server.
8. If the Application Server is listed, exit the dialog by clicking **Cancel**.

   No additional configuration is required, and the IMPAX Client now uses Windows Authentication for logging in.

   or

   If the Application Server is not listed, continue with step 9.
9. In the **Add this Web site to the zone** field, type or paste the URL of the Application Server.
10. Click **Add**.
11. Click **Close**.

    The IMPAX Client now uses Windows Authentication for logging in.

Adding additional Application Servers to the IMPAX cluster

(Topic number: 11333)

Add an additional Application Server to the cluster to distribute information requests to multiple servers. When requests are distributed to multiple servers, the workload for each server can be equalized and does not overburden one particular server.

Important!

All Application Servers in a cluster must be running the same version of the Windows operating system. Therefore, any additional servers that you add to the cluster must be running the same version of Windows as the existing servers.

To add an additional Application Server to the IMPAX cluster

1. Import the SSL Certificate from the primary Application Server.

   For details about how to import an SSL Certificate, refer to "Copying an SSL certificate to another Application Server" (topic number 11427) in the *IMPAX 6.5.1 Application Server Knowledge Base*.
2. Install the Application Server software according to *Installing the IMPAX Business Services* (refer to page 49).
3. Import the portable password file onto the secondary Application Server.

   Details are available in *Importing the portable password file* (refer to page 55).

4. On a Windows 2003 Application Server, open **Control Panel** and select **Add/Remove Programs**.

   or

   On a Windows 2008 Application Server, open **Control Panel** and select **Programs and Features**.

5. On a Windows 2003 Application Server, on the Add/Remove Programs screen, select **ADAM**. Click **Remove**.

   or

   On a Windows 2008 Application Server, on the Programs and Features screen, right-click **AD LDS Instance AgfaHealthcare** and click **Uninstall**.

6. Accept all defaults, if any, and remove the ADAM or AD LDS instance.
7. On the secondary Application Server, create a replica of the primary Application Server ADAM database (Windows 2003), or the primary Application Server AD LDS database. Details are available in *Replicating ADAM* (refer to page 92) and in *Replicating AD LDS* (refer to page 93).
8. In the IMPAX Client, Configure area, modify the paths of any web services that will be accessed on the new Application Server.

   For instructions on modifying the paths to web services, refer to "Configuring access to images using storage groups" (topic number 9398) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Replicating ADAM

(Topic number: 11380)

All IMPAX user information is stored in the ADAM database. To ensure that there is always an ADAM instance available to authenticate users on the Clients, create a replica copy of the ADAM database on a second Application Server. After configuring the ADAM replica, the ADAM database is replicated every 15 seconds between the two ADAM instances.

Follow this procedure when replicating an ADAM database on another Windows 2003 server.

Note:

You must be an administrator user in Windows on the Application Server with the original ADAM instance or a domain user to create a replica of the ADAM database.

To replicate ADAM

1. Setup the additional Application Server.
2. From the Microsoft website, download and run the ADAM executable file **ADAMSP1_X86_English.exe**.

   The ADAM software is installed.

3. Select **Start** > **Programs** > **ADAM** > **Create an ADAM Instance**.
4. In the Welcome dialog, click **Next**.
5. In the Setup Options dialog, select **A replica of an existing instance**. Click **Next**.

6. In the Instance name dialog, type **AgfaHealthcare**.

   The name of the replicated instance must be the same as the original instance.

7. Click **Next**.
8. In the Ports dialog, accept the default LDAP port number (389) and SSL port number (636). Click **Next**.
9. In the Joining a Configuration Set dialog, type the **fully qualified domain name** and **LDAP port number** of the ADAM instance to be replicated. Click **Next**.
10. In the Administrative Credentials dialog, select **This Account.**
11. Select the **Agfaservice** account and type the password. Click **Next**.

    This account must have domain administrator privileges. If it does not have these privileges, select an account that does.

12. In the Copying Application Directory Partitions dialog, select all the available partitions and click **Add**. Click **Next**.
13. In the Data files and Data recovery files fields, leave the default file locations. Click **Next**.
14. In the Service Account Selection dialog, select **Network Service Account**. Click **Next**.
15. If a confirmation message appears, click **Yes**.
16. In the ADAM Administrators dialog, select **Current logged on user** (the user must have domain administrator privileges) for the ADAM administrator. Click **Next**.
17. In the Ready to Install dialog, click **Next**.

    The ADAM is installed, and the instance is replicated.

18. When the installation is complete, click **Finish**.

Replicating AD LDS

(Topic number: 115221)

On Application Servers running Windows Server 2008, all IMPAX user information is stored in the AD LDS database. To ensure that there is always an AD LDS instance available to authenticate users on the Clients, create a replica of the AD LDS database on a second Windows 2008 Application Server. After configuring the AD LDS replica, the AD LDS database is replicated every 15 seconds between the two AD LDS instances.

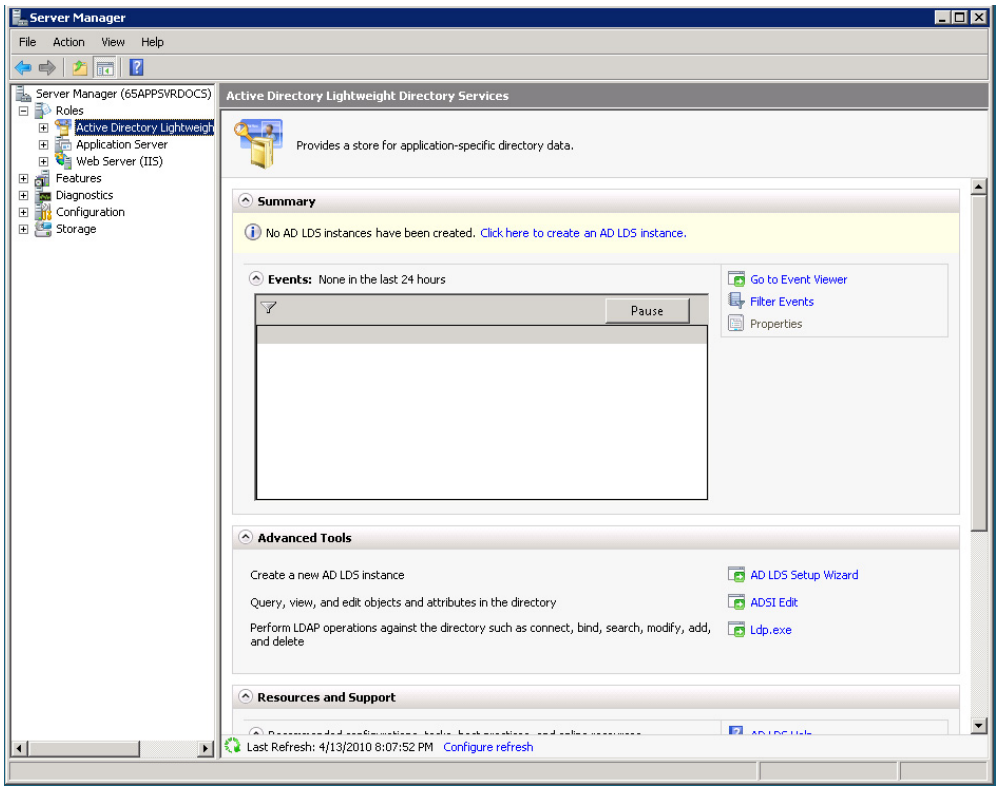
Note:

To perform the replication, you can use either a Windows domain Administrator account, or, if the domain Administrator account is not available, you can add an account with limited privileges to the Administrator group. For instructions on how to add an account with limited privileges to the Administrator group, see Adding a user account to the Administrator group (refer to page 108).

To replicate AD LDS

1. Set up the additional Application Server running Windows Server 2008.

2. Ensure that AD LDS is installed on the server you set up in Step 1.
3. Log into the new server.
4. Select **Start** > **Server Manager**.
5. Under **Roles**, select **Active Directory Lightweight Services**.



6. Under **Advanced Tools**, click **AD LDS Setup Wizard**. .
7. In the Active Directory Lightweight Directory Services dialog, click **Next**.
8. In the Setup Options dialog, select **A replica of an existing instance**, then click **Next**.
9. In the Instance Name dialog, type **AgfaHealthcare**.

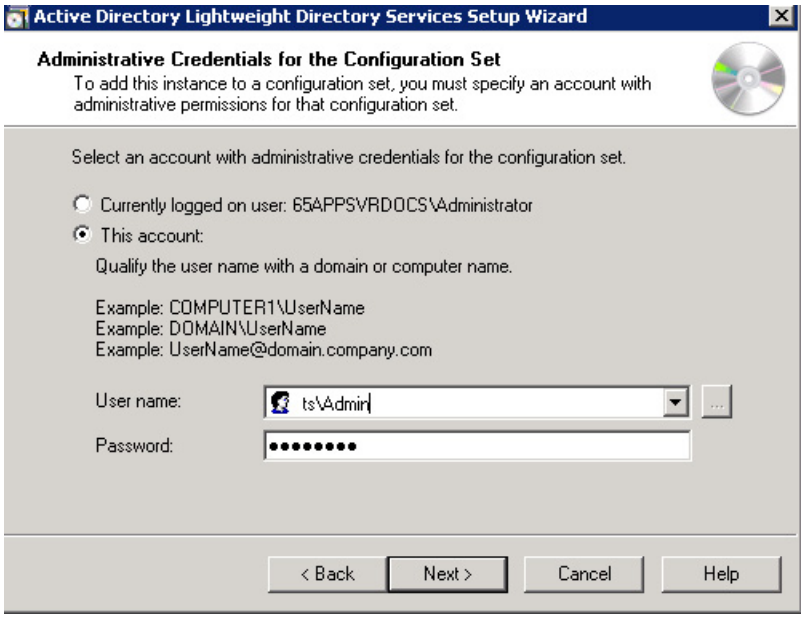
Important!

The name of the replicated instance must be identical to the original instance.

10. Click **Next**.
11. In the Ports dialog, accept the default LDAP port number (389) and SSL port number (636) and click **Next**.
12. In the Joining a Configuration Set dialog, type the **fully qualified domain name** and **LDAP port number** of the AD LDS LDAP instance to be replicated.
13. Click **Next**.
14. In the Administrative Credentials for the Configuration Set dialog, select **This Account.**

15. In the **User Name** text box, enter ***domain\Agfaservice account*** where *domain* is the network domain and *Admin* is the account password.

    In the following illustration, *ts* is the domain and *Admin* is the administrator account.



16. In the **Password** text box, enter the password for the account you specified in the previous step.
17. Click **Next**.
18. In the Copying Application Directory Partitions dialog, select the **CN=healthcare,DC=agfa,DC=com** partition and click **Next**.
19. In the File Locations dialog, in the **Data Files** and **Data Recovery files** text boxes, enter

    C:\Program Files\Microsoft ADAM\AgfaHealthcare\data
20. In the Service Account Selection dialog, select **Network Service Account**. Click **Next**

    If a confirmation message is displayed, click **Yes**.
21. In the AD LDS Administrators dialog, select **Currently logged on user**.
22. Click **Next**.
23. In the Ready to Install dialog, click **Next**.

    The AD LDS instance is installed, and the instance is replicated.

> **Note:**
>
> The installation process takes a few minutes to complete.

24. When the installation is complete, click **Finish**.

7 Migrating an Application Server from a Windows 2003 server to a Windows 2008 server

All Application Servers in the same cluster must be running the same operating system—either Windows Server 2003 or Windows Server 2008. When migrating from Windows 2003 to Windows 2008, you must replicate the ADAM data on the Windows 2003 server to the AD LDS database on the new Windows 2008 server.

Data replication can take place when both the Windows 2003 and Windows 2008 Application Server belong to the same domain, or when both servers are part of a workgroup.

Migrating from Windows 2003 to Windows 2008 within a domain

(Topic number: 119950)

You can migrate ADAM data from the Windows 2003 Application Server to the AD LDS database on a new Windows 2008 Application Server when both servers belong to a domain.

Migrating from Windows 2003 to Windows 2008: Prerequisite tasks

(Topic number: 119953)

Before migrating ADAM data on a Windows 2003 server to the AD LDS database on a Windows 2008 server, the following tasks must be performed.

To migrate from Windows 2003 to Windows 2008

1. Install Windows 2008 on a new server.
2. Install IMPAX Business Services on the Windows 2008 Server.
3. Bring the Windows 2008 Application Server into the cluster.
4. Disable the firewall on the Windows 2003 Application Server you are using for the ADAM to AD LDS replication.
5. Disable the firewall on the new Windows 2008 server.
6. Run a healthcheck to ensure that the Windows 2008 server is functioning correctly.

Removing the AgfaHealthcare AD LDS instance

(Topic number: 113480)

Before starting the migration process from Windows Server 2003 to Windows Server 2008, remove the AgfaHealthcare AD LDS instance from the Windows 2008 Application Server.

To remove the AgfaHealthcare AD LDS instance

1. Log into the Windows 2008 Application Server.
2. Open a command prompt.
3. To change to the IMPAXAdam directory, type

   cd C:\Program Files\Agfa\IMPAX Business Services\IMPAXAdam
4. Type

   IMPAXAdam -remove
5. When the command prompt displays a warning message, type

   y

The AgfaHealthcare AD LDS instance is removed from the Windows 2008 Application Server.

Replicating the ADAM database on the Windows 2008 server

(Topic number: 109637)

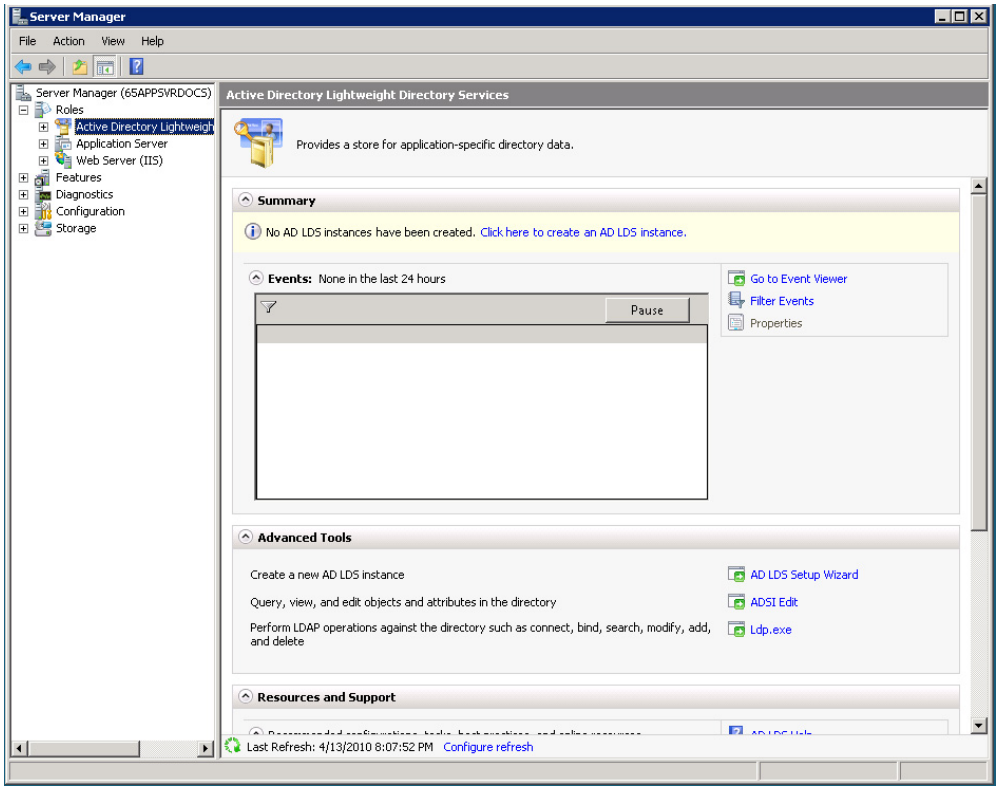
When migrating from a Windows 2003 Application Server to a Windows 2008 Application Server, you must replicate the existing ADAM LDAP database on the Windows 2008 server.

Note:

To perform the replication, you can use either a Windows domain Administrator account, or, if the domain Administrator account is not available, you can add an account with limited privileges to the Administrator group. For instructions on how to add a Windows account with limited privileges to the Administrator group, see the section Adding a limited account to the Administrator group (refer to page 108).

To replicate the ADAM database on the Windows 2008 server

1. Log into the Windows Server 2008 server that you are bringing into the cluster.
2. Select **Start** > **Server Manager**.
3. Expand the **Roles** node and elect **Active Directory Lightweight Services**.



4. Under Advanced Tools, click **AD LDS Setup Wizard**.
5. On the Active Directory Lightweight Directory Services screen, click **Next**.
6. On the Setup Options screen, select **A replica of an existing instance**. Click **Next**.
7. In the Instance Name dialog, type **AgfaHealthcare**.

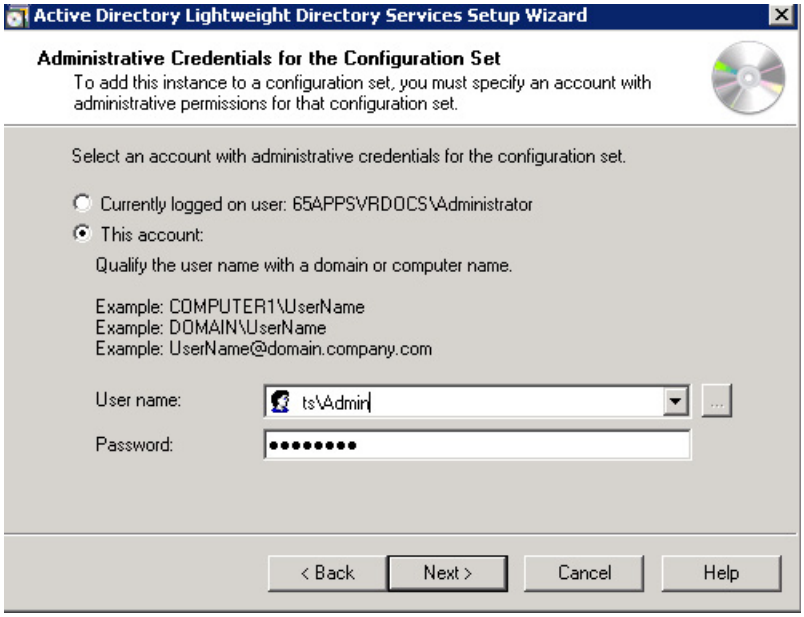
Important!

The name of the replicated instance must be identical to the original instance.

8. Click **Next**.

9. On the Ports screen, accept the default LDAP port number (389) and SSL port number (636). Click **Next**.
10. On the Joining a Configuration Set screen, type the fully qualified domain name and LDAP port number of the ADAM LDAP instance (the Windows 2003 ADAM server) that you are using for the replication. Click **Next**.
11. On the Administrative Credentials for the Configuration Set screen, select **This Account.**
12. In the User Name field, type ***domain\Agfaservice_account,*** where *domain* is the network domain and *Agfaservice_account* is the account user name.

    In the following illustration, *ts* is the domain and *Admin* is the administrator account.



13. In the Password field, enter the password for the account you specified in the previous step. Click **Next**.
14. On the Copying Application Directory Partitions screen, select the **CN=healthcare,DC=agfa,DC=com** partition. Click **Next**.
15. On the File Locations screen, in the Data Files and Data Recovery files fields, type

    C:\Program Files\Microsoft ADAM\AgfaHealthcare\data. Click **Next**.
16. On the Service Account Selection screen, select **Network Service Account**. Click **Next**.

    If a confirmation message is displayed, click **Yes**.
17. On the AD LDS Administrators screen, select **Currently logged on user**. Click **Next**
18. On the Ready to Install screen, click **Next**.

    The installation process takes a few minutes to complete.
19. When the installation is complete, click **Finish**.

Transferring the primary LDAP instance from Windows Server 2003 to Windows Server 2008

(Topic number: 110097)

As part of the migration from a Windows 2003 Application Server to a Windows 2008 Application Server, transfer both the primary schema master role and naming master role to the new Windows 2008 Application Server.

Transferring the schema master role from the Windows 2003 server to the Windows 2008 server

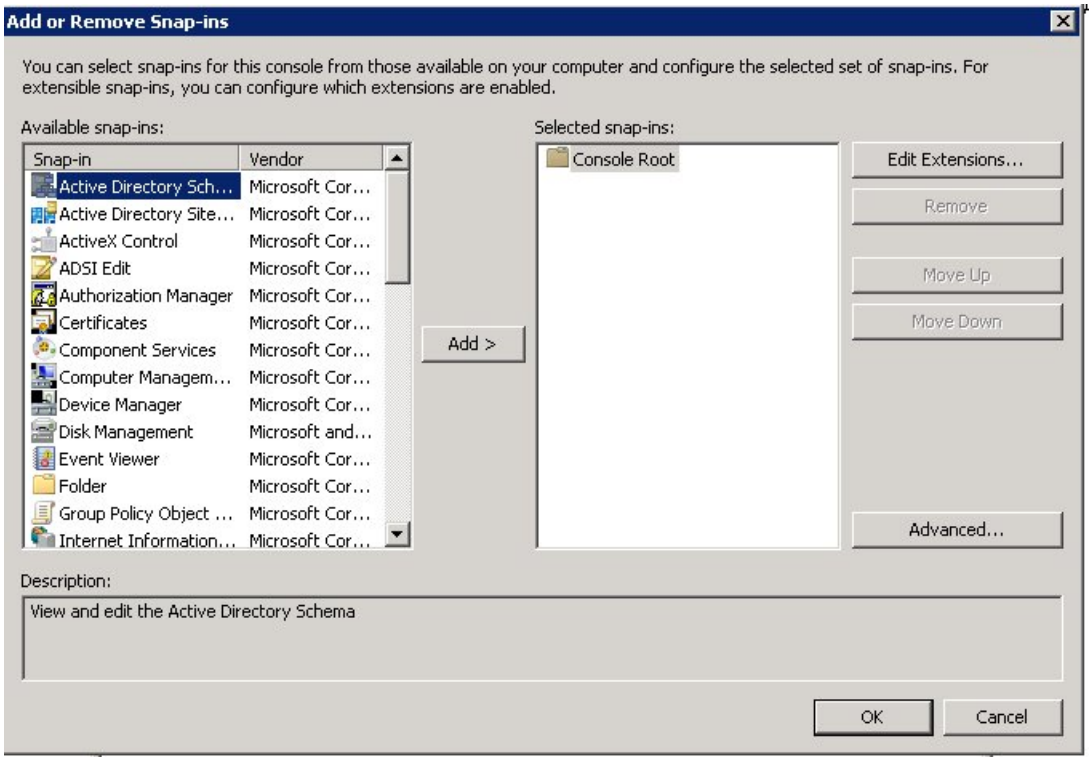
(Topic number: 110077)

The first step in switching the primary LDAP instance from the Windows 2003 server to the Windows 2008 server is to transfer the schema master to the Windows 2008 Application Server.

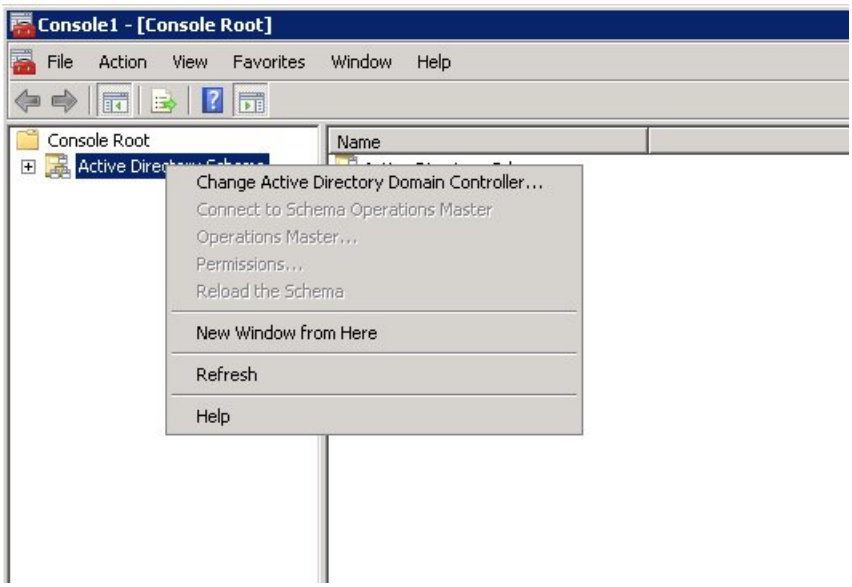
To transfer the schema master role from the Windows 2003 server to the Windows 2008 server

1. Log into the new Windows 2008 Application Server on which you performed the AD LDS replication.
2. Open a command prompt.
3. Change to the **Windows\System 32** directory.
4. To register the schmmgmt.dll, type

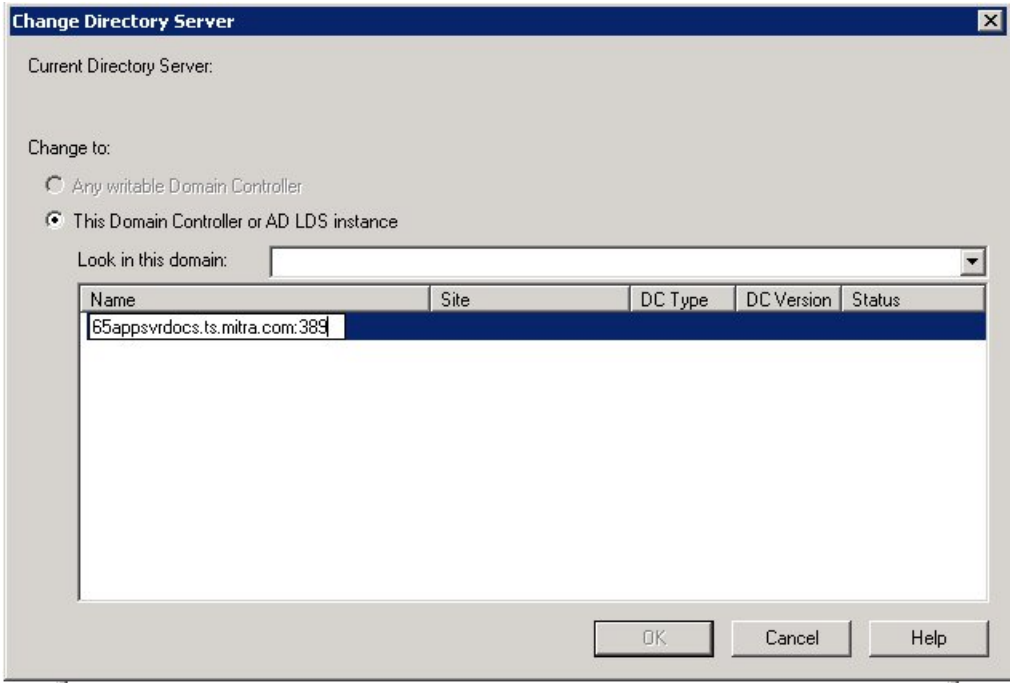
   regsvr32 schmmgmt.dll
5. Select **Start** > **Run**.
6. In the Run dialog, type **mmc**. Click **OK.**
7. Select **File** > **Add/Remove Snap-in**.
8. In the Add or Remove Snap-ins dialog, from the Available Snap-ins list, select **Active Directory Schema**



9. Click **Add**, then click **OK**.
10. Right-click **Active Directory Schema**, and select **Change Active Directory Domain Controller**



11. Click **This Domain Controller or AD LDS instance**.
12. Under Name, enter the name, the domain, and port number of the Windows 2008 replica.



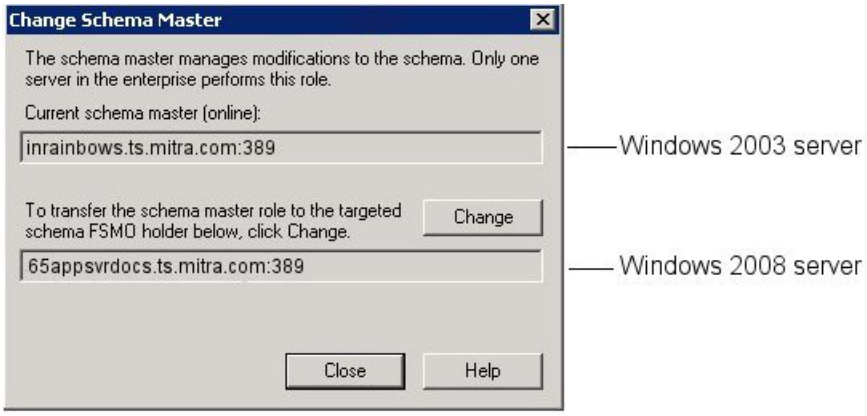
13. Click **OK**.

    A dialog is displayed informing you that the Active Directory Schema snap-in is not connected to the schema operations master.

14. Click **OK**

15. Right-click **Active Directory Schema** and select **Operations Master**.

    The Change Schema Master dialog is displayed. The current schema master (the Windows 2003 server), is shown in the Current Schema Master (online) field. The Windows 2008 server you specified in Step 12 is shown in the lower field as shown in the following illustration.



16. Click **Change**.

    A confirmation dialog is displayed, informing you that the Operations Master was successfully transferred from the Windows 2003 server to the Windows 2008 server.

17. Click **Close**.

Transferring the domain naming master role to the Windows 2008 Application Server

(Topic number: 110090)

As part of the migration from a Windows 2003 Application Server to a Windows 2008 Application Server, you must transfer the domain naming master role to the Windows 2008 Application Server.

To transfer the domain naming master role to the Windows 2008 Application Server

1. Log into the Application server running Windows Server 2008.
2. Open a command prompt and type

   dsmgmt
3. At the dsmgmt command prompt, type

   roles
4. At the fsmo maintenance command prompt, type

   connections
5. At the server connections command prompt, type

   connect to server *servername:portnumber*

   where *servername* is the name of the AD LDS instance to use as the new naming master, and *portnumber* is the communications port number on that server.
6. Type **quit**.
7. At the fsmo maintenance command prompt, type

   transfer naming master
8. In the Role Transfer dialog, click **Yes**.
9. At the fsmo maintenance command prompt, type **quit**.
10. At the dsmgmt command prompt, type **quit**.

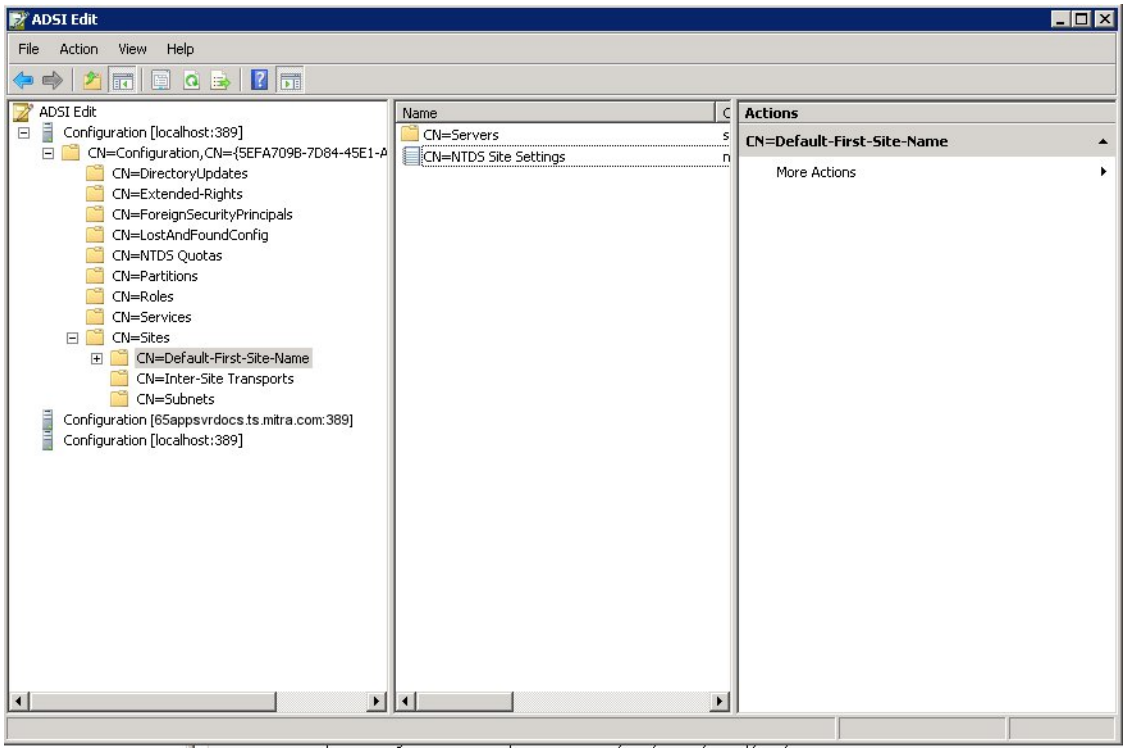
Setting up replication to repeat every 15 minutes

(Topic number: 113465)

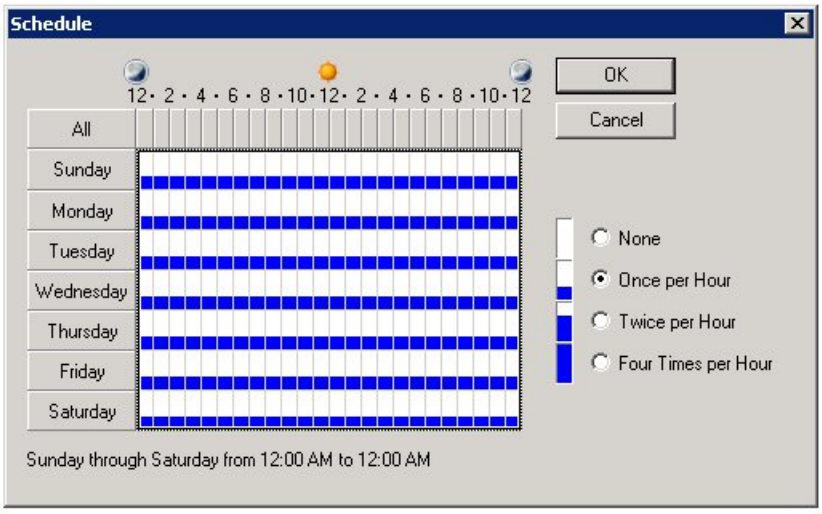
So that data remains consistent between all databases in the cluster, set up replication between AD LDS instances to occur every 15 minutes.

To set up replication to repeat every 15 minutes.

1. Log into the Windows 2008 Application Server.
2. Launch **ADSI Edit**.
3. In the left-hand pane, expand **CN=Sites**, and click **Cn=Default-First-Site-Name**.



4. In the center pane, right-click **CN=NTDS Site Settings** and select **Schedule**.
5. In the **CN=NTDS Site Settings** dialog, scroll down to the schedule attribute.
6. To set the database to replicate every hour of every day at 15 minute intervals, click **Four Times per Hour**.



7. Click **OK**.

Migrating web services plugins to the Windows 2008 Application Server

(Topic number: 120616)

When migrating from a Windows 2003 Application Server to a Windows 2008 Application Server, you must migrate the web services plugins that are used for LDAP Enterprise Authentication.

To migrate web services plugins to the Windows 2008 Application Server

1. Log into the Windows 2003 Application Server that you are using for the migration and navigate to **E:\inetpub\wwwroot\AgfaHC.User.Security.Web.Services**.
2. Open the **web.config** file.
3. Find the PluginSettings section of the file and copy it into a text editor such as Notepad and save the file.
4. Log into the Windows 2008 Application Server and navigate to **E:\inetpub\wwwroot\AgfaHC.User.Security.Web.Services**.
5. Open the **web.config** file.
6. Find the PluginSettings section of the file and replace it with the PluginSettings section from the Windows 2003 server you copied in step 3.
7. Save the modified **web.config** file.
8. Repeat steps 1-7 using the web.config files in the E:\inetpub\wwwroot\AgfaHC.User.Administration.Web.Services directory on the Windows 2003 and Windows 2008 Application Servers.

Updating the database server's map_ini table

(Topic number: 118595)

Update the ini_value in the database server's map_ini table to the name of the replica (Windows 2008) Application Server.

To update the database server's map_ini table

1. Open a SQL editor such as clui.
2. To check the current value of the map_ini table's ini_value field, type

   select ini_value from map_ini where ini_key like '%ws.authenticate.uri%'
3. If the query you ran in the previous step returns the name of the Windows 2003 Application Server used for replication, type

   update map_ini set ini_value=https://*Windows 2008 server*/AgfaHC.User.Security.Web.Services/Login.asmx where ini_section=SERVICE_TOOLS ini_key=ws.authenticate.uri

   where *Windows 2008 server* is the fully qualified domain name of the replicated Windows 2008 server.

The value of the map_ini table's ini_value field is the name of the replica (Windows 2008) Application Server.

Updating the hostname in the Agfa Security Wizard

(Topic number: 118597)

You must use the Agfa Security Wizard to update the hostname on the replicated Windows 2008 Application Server.

To update the hostname in the Agfa Security Wizard

1. Log into the Windows 2008 Application Server.
2. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
3. In the Security Wizard, select **Work with the Application Server default settings** and click **Next**.
4. In the Web Services Url Configuration dialog, in the Hostname field, enter the name of the replica Windows 2008 Application Server and click **Update**. Click **Next**.
5. In the User Management dialog, if you want to add an Administrator, select **Add Administrator** and enter a user name and password into the User Name and Password fields

   or

   If you do not want to add an Administrator, select **Do not add Administrator**.
6. Click **Next**.
7. Select either **Add Administration License** and specify a license file, or select **No Administration License**.
8. Click **Finish**.
9. Close the Agfa Security Wizard.

Verifying that the Internet station container is updated with the Windows 2008 Application Server

(Topic number: 118873)

To complete the replication, you should verify that the Internet [Default] station container in the IMPAX Client is updated with the new, replicated Windows 2008 IMPAX.

To verify that the Internet station container is updated with the Windows 2008 IMPAX,

1. Open the IMPAX Client.
2. From the **Configure** drawer menu  , select **Stations**.

   or

   Or, from the List area bar, click the User ID menu and select **Station Configuration**.
3. Expand the Internet [Default] station container.

4. Verify that the newly replicated Windows 2008 IMPAX is listed.

Removing the original ADAM instance from the replication set

(Topic number: 110092)

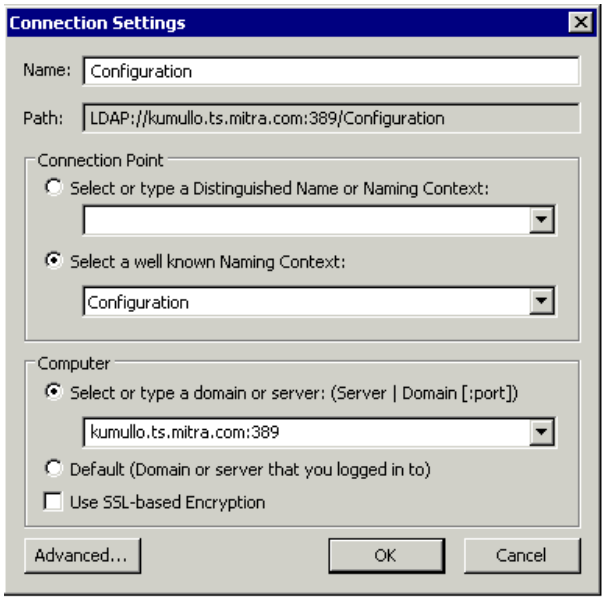
You must delete the original AgfaHealthcare entry from the replication set on the Windows 2008 Application Server.

To remove the original ADAM instance from the replication set

1. Ensure that the ADAM instance on the Windows 2003 Application Server is uninstalled and offline.
2. On the primary AD LDS instance, open the ADSI Edit snap-in.

> **Note:**
>
> If you have not set up a configuration connection to the Windows 2003 server, continue with step 3. If you have already created a configuration connection, skip ahead to step 8.

3. In the left pane of ADSI Edit, right-click **ADSI Edit** and select **Connect to**
4. In the Connection Settings dialog, in the Name field, type **Configuration**.



5. Select **Select a well known Naming Context** and from the list, select **Configuration**.
6. Type the name of the Windows 2008 server to create a connection configuration for.
7. Click **OK**.
8. In the left pane in ADSI Edit, select the **Configuration** connection.
9. Navigate to **CN=Configuration** > **CN=Sites** > **CN=Default-First-Site-Name** > **CN=Servers**.

10. Find a folder with the name of the Windows 2003 server used for replication and delete it.

Important!

Enable the Windows firewall on the Windows 2008 Application Server.

You can now re-image the Windows 2003 server with Windows Server 2008 and bring the machine into the cluster.

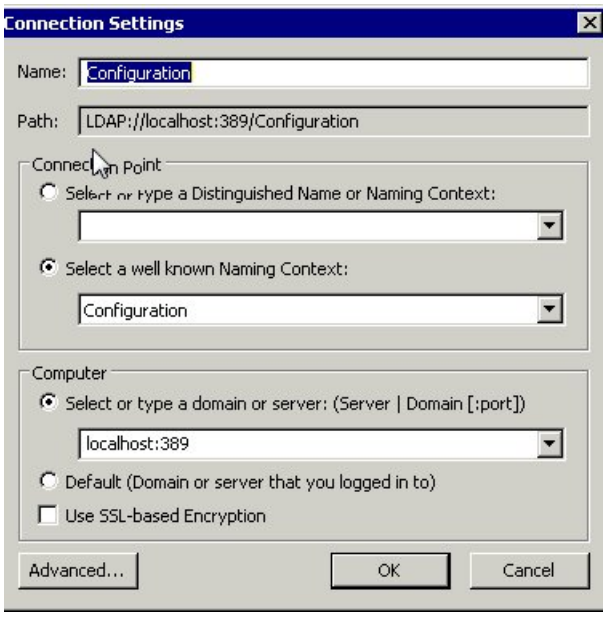
Adding a limited Windows account to the Administrator group in Windows Server 2008

(Topic number: 109263)

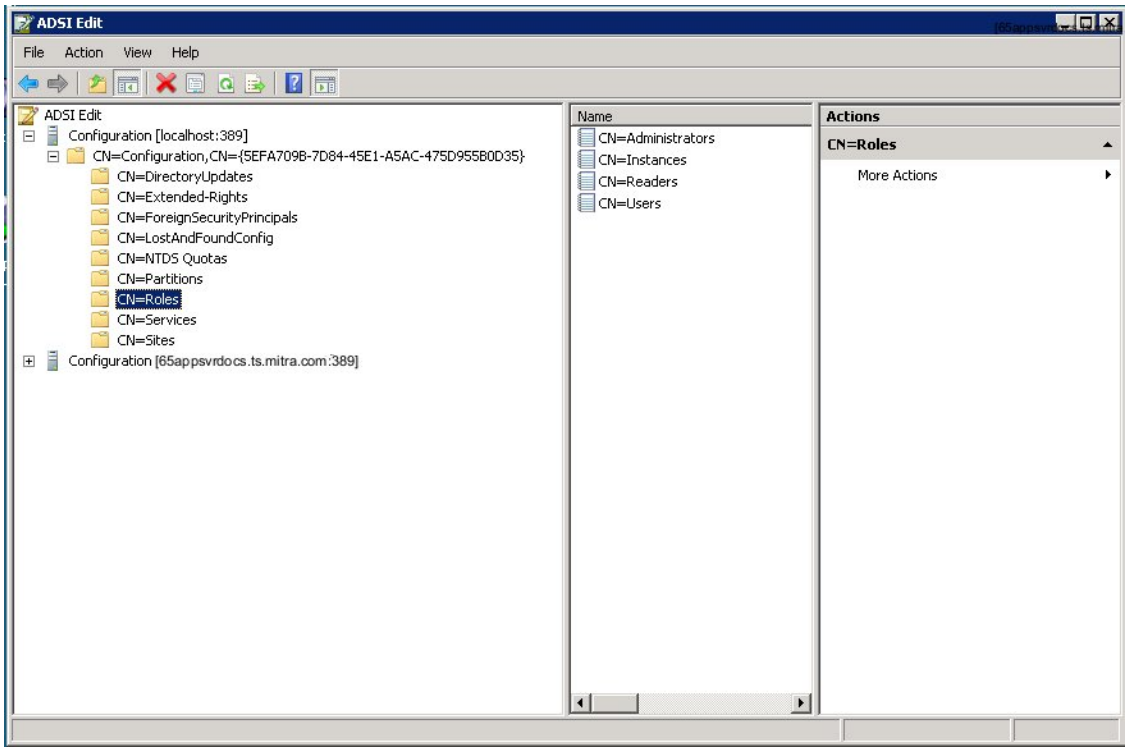
When replicating an ADAM or AD LDS instance, it may be not be practical to use the domain Administrator account. Alternatively, you can add a limited Windows account to the Administrator group before performing the replication.

To add a limited Windows account to the Administrator group in Windows Server 2008

1. Log into the Application Server running Windows Server 2008.
2. Select **Start** > **Server Manager**.
3. In the left-hand pane, expand the **Roles** node and click **Active Directory Lightweight Directory Services**.
4. In the right-hand pane, find the **Advanced Tools** section and click **ADSI Edit**.
5. In the ADSI editor, create a connection to an AD LDS instance.
    a. Right-click **ADSI Edit** in the left-hand pane and select **Connect To**.
    b. Enter values into the Connection Settings dialog as shown in the image that follows and click **OK**.



6. Add the current user account to the Administrator group.
   a. Under the **ADSI Edit** node, expand **Configuration** [**localhost:389**] and click **CN=Roles**.

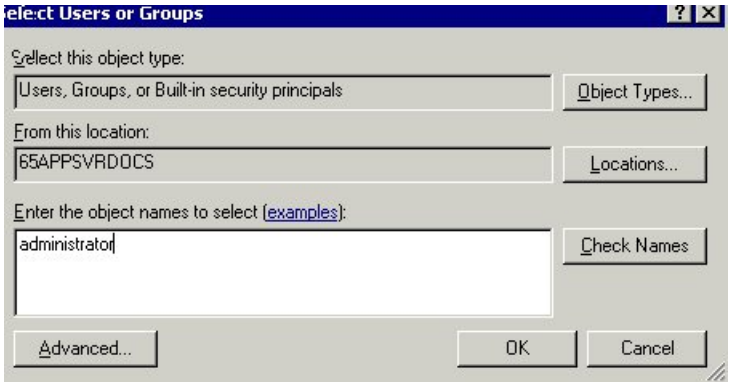


   b. In the center pane, right-click the **CN=Administrators** role and from the drop-down menu, select **Properties**.
   c. In the CN=Administrators Properties dialog, scroll down to the **member** attribute and click **Edit**.

The Multi-valued Distinguished Names With Security Principal Editor dialog is displayed, showing the list of users associated with the member attribute.

d. Click **Add Windows Account**.

e. In the Select Users or Groups dialog, type **administrator** and then click **OK**.



The account name appears in the Multi-valued Distinguished Name With Security Principal Editor dialog as a member of the Administrator group.

f. Click **OK** twice to return to ADSI Edit.

Migrating from Windows 2003 to Windows 2008 within a workgroup

(Topic number: 119910)

You can migrate ADAM data from the Windows 2003 Application Server to the AD LDS database on a new Windows 2008 Application Server when both servers belong to a workgroup.

Migrating from Windows 2003 to Windows 2008: Prerequisite tasks

(Topic number: 119953)

Before migrating ADAM data on a Windows 2003 server to the AD LDS database on a Windows 2008 server, the following tasks must be performed.

To migrate from Windows 2003 to Windows 2008

1. Install Windows 2008 on a new server.
2. Install IMPAX Business Services on the Windows 2008 Server.
3. Bring the Windows 2008 Application Server into the cluster.
4. Disable the firewall on the Windows 2003 Application Server you are using for the ADAM to AD LDS replication.
5. Disable the firewall on the new Windows 2008 server.

6. Run a healthcheck to ensure that the Windows 2008 server is functioning correctly.

Removing the AgfaHealthcare AD LDS instance

(Topic number: 113480)

Before starting the migration process from Windows Server 2003 to Windows Server 2008, remove the AgfaHealthcare AD LDS instance from the Windows 2008 Application Server.

To remove the AgfaHealthcare AD LDS instance

1. Log into the Windows 2008 Application Server.
2. Open a command prompt.
3. To change to the IMPAXAdam directory, type

   cd C:\Program Files\Agfa\IMPAX Business Services\IMPAXAdam
4. Type

   IMPAXAdam -remove
5. When the command prompt displays a warning message, type

   y

The AgfaHealthcare AD LDS instance is removed from the Windows 2008 Application Server.

Applying the Microsoft hotfix to the Windows 2003 Application Server

(Topic number: 119912)

To enable ADAM to AD LDS replication in a workgroup, you must download Microsoft hotfix KB973678 and apply the hotfix to the Windows 2003 server you are using for the ADAM replication.

To apply the Microsoft hotfix to the Windows 2003 Application Server

1. Open a web browser and navigate to the following web address:

   http://support.microsoft.com/kb/973678
2. Download and install the Microsoft hotfix KB973678 on the Windows 2003 Application Server that you are using for the ADAM replication.

Editing the Windows 2003 registry

(Topic number: 119928)

Before replicating the Windows 2003 ADAM data on a Windows 2008 server, you must edit the Windows 2003 registry.

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 edit the Windows 2003 registry

1. On the Windows 2003 server, select **Start** > **Run**.
2. In the Run dialog, type

   regedit
3. In the Registry Editor, expand **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Services** > ***ADAM instance name*** > **Parameters**.

   where *ADAM instance name* is the name of the ADAM instance that you are replicating.
4. Right-click anywhere in the right pane of the registry editor and select **New** > **DWORD Value**.
5. Enter the name for the new registry key by typing

   NTLMSessionKey
6. Right-click the registry value you created and select **Modify**.
7. In the Edit DWORD Value dialog, select **Hexadecimal** and in the Value data field, type

   1
8. Click **OK**.

   The DWORD value is set to 0x00000001 in the Data column.

Changing the logon account to AgfaService

(Topic number: 119933)

On the Windows 2003 server whose ADAM data you are replicating on a Windows 2008 server, you must change the logon account to AgfaService.

To change the logon account to AgfaService

1. Select **Start** > **Administrative Tools** > **Services**.
2. In the list of services, double-click **AgfaHealthcare**.
3. Click **Stop**.
4. Select the Log On tab.
5. Change the Logon Account to AgfaService.
6. Enter the password for the AgfaService account.
7. Click **OK**.
8. Restart the AgfaHealthcare service.

Setting the msDS-ReplAuthenticationMode attribute

(Topic number: 119938)

Before starting the ADAM to AD LDS replication, on the Windows 2003 Application Server you are using for the replication, set the msDS-ReplAuthenticationMode attribute.

To set the msDS-ReplAuthenticationMode attribute

1. On the Windows 2003 Application Server, launch **ADSI Edit**.
2. In the left pane of the ADSI Edit snap-in, expand the configuration.
3. Right-click the **CN=Configuration** folder and select **Properties**.

   The Attribute Editor dialog opens.
4. Select the msDS-ReplAuthenticationMode attribute and click **Edit**.

   The Integer Attribute Editor dialog opens.
5. In the Value field, enter **0** as the value.
6. Click **OK** to close the Integer Attribute Editor dialog.
7. Click **OK** to close the Attribute Editor.

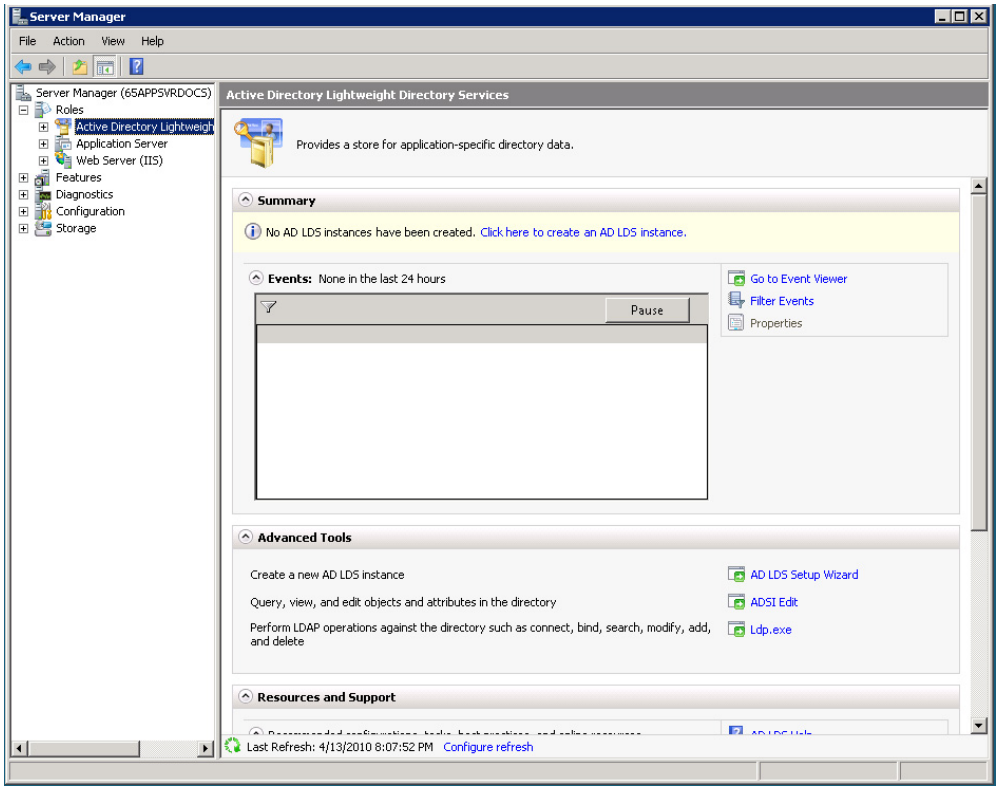
Replicating the ADAM database on the Windows 2008 server in a workgroup

(Topic number: 119940)

When migrating from a Windows 2003 Application Server to a Windows 2008 Application Server, you must replicate the existing ADAM LDAP database on the Windows 2008 server.

To replicate the ADAM database on the Windows 2008 server in a workgroup

1. Log into the Windows Server 2008 server that you are bringing into the cluster.
2. Select **Start** > **Server Manager**.
3. Expand **Roles** node and select **Active Directory Lightweight Services**.



4. Under Advanced Tools, click **AD LDS Setup Wizard**.
5. In the Active Directory Lightweight Directory Services screen, click **Next**.
6. In the Setup Options dialog, select **A replica of an existing instance**. Click **Next**.
7. In the Instance Name dialog, type **AgfaHealthcare**.

Important!

The name of the replicated instance must be identical to the original instance on the Windows 2003 server used for replication.

8. Click **Next**.
9. In the Ports screen, accept the default LDAP port number (389) and SSL port number (636). Click **Next**.
10. In the Joining a Configuration Set screen, type the fully qualified domain name and LDAP port number of the ADAM LDAP instance (the Windows 2003 ADAM server) that you are using for the replication.
11. In the Administrative Credentials for the Configuration Set screen, accept the default value **Currently logged on user**. Click **Next.**
12. In the File Locations screen, in the Data Files and Data Recovery files fields, accept the default settings and click **Next**.
13. Click **Next**.

14. In the Copying Application Directory Partitions screen, select the **CN=healthcare,DC=agfa,DC=com** partition. Click **Next**.
15. On the Service Account Selection screen, select **This account** and click **Browse**.
16. In the Select User screen, under Enter the object name to select, type **AgfaService**. Click **Check Names** and then click **OK**.
17. In the Service Account Selection screen, type the password for the AgfaService account. Click **Next**.

    If a confirmation message is displayed, click **Yes**.
18. On the AD LDS Administrators screen, accept the default values. Click **Next**
19. On the Ready to Install screen, click **Next**.

    The installation process takes a few minutes to complete.
20. When the installation is complete, click **Finish**.

Transferring the primary LDAP instance from Windows Server 2003 to Windows Server 2008

(Topic number: 121810)

As part of the migration from a Windows 2003 Application Server to a Windows 2008 Application Server, transfer the primary schema master role to the new Windows 2008 Application Server.

Transferring the schema master role from the Windows 2003 server to the Windows 2008 server

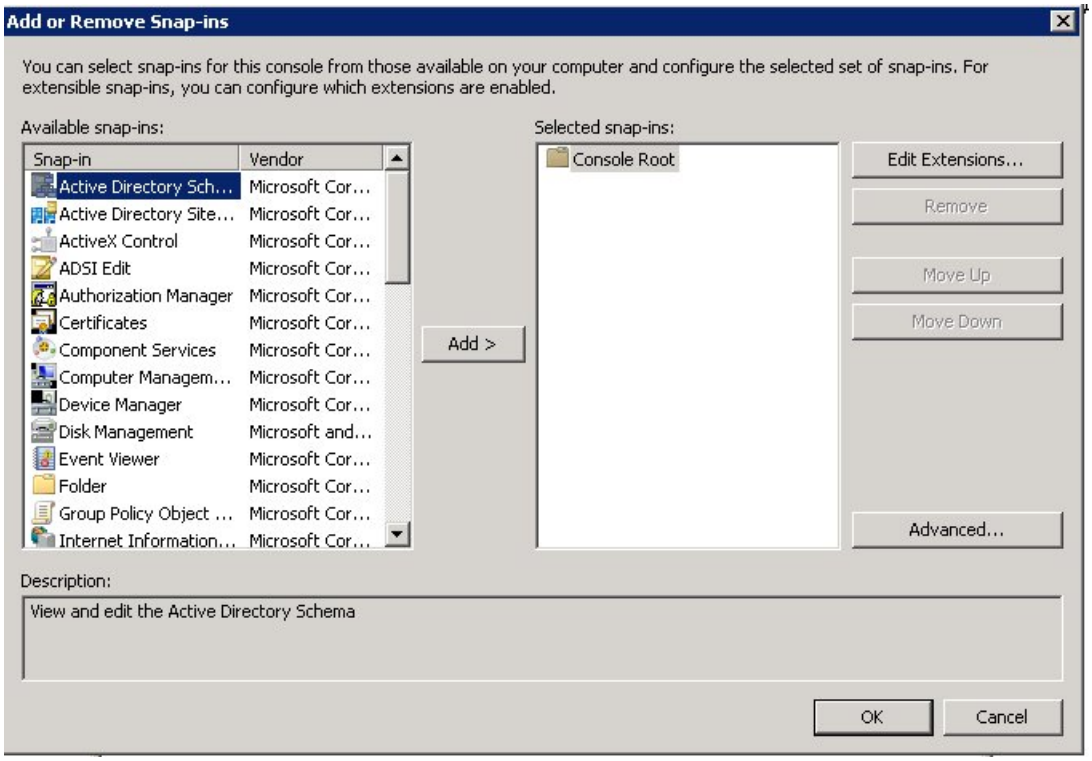
(Topic number: 110077)

The first step in switching the primary LDAP instance from the Windows 2003 server to the Windows 2008 server is to transfer the schema master to the Windows 2008 Application Server.

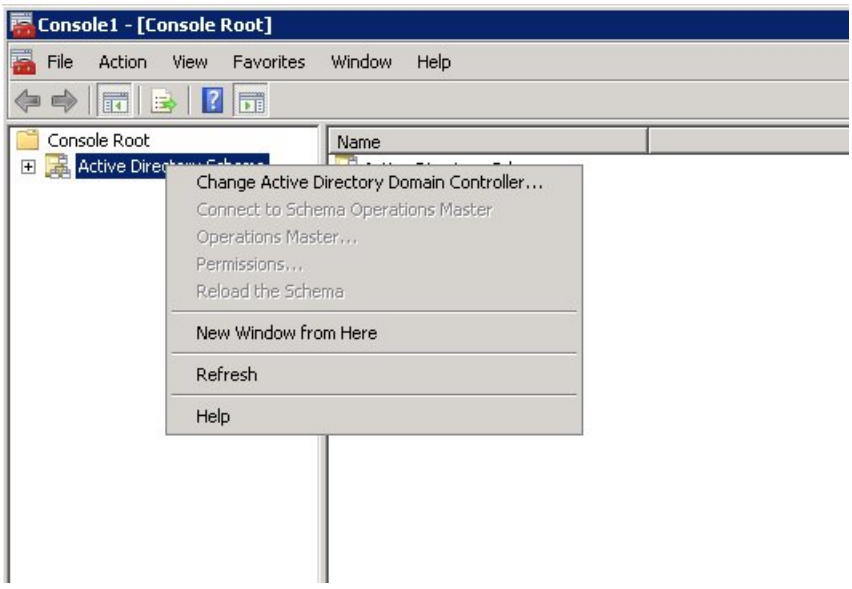
To transfer the schema master role from the Windows 2003 server to the Windows 2008 server

1. Log into the new Windows 2008 Application Server on which you performed the AD LDS replication.
2. Open a command prompt.
3. Change to the **Windows\System 32** directory.
4. To register the schmmgmt.dll, type

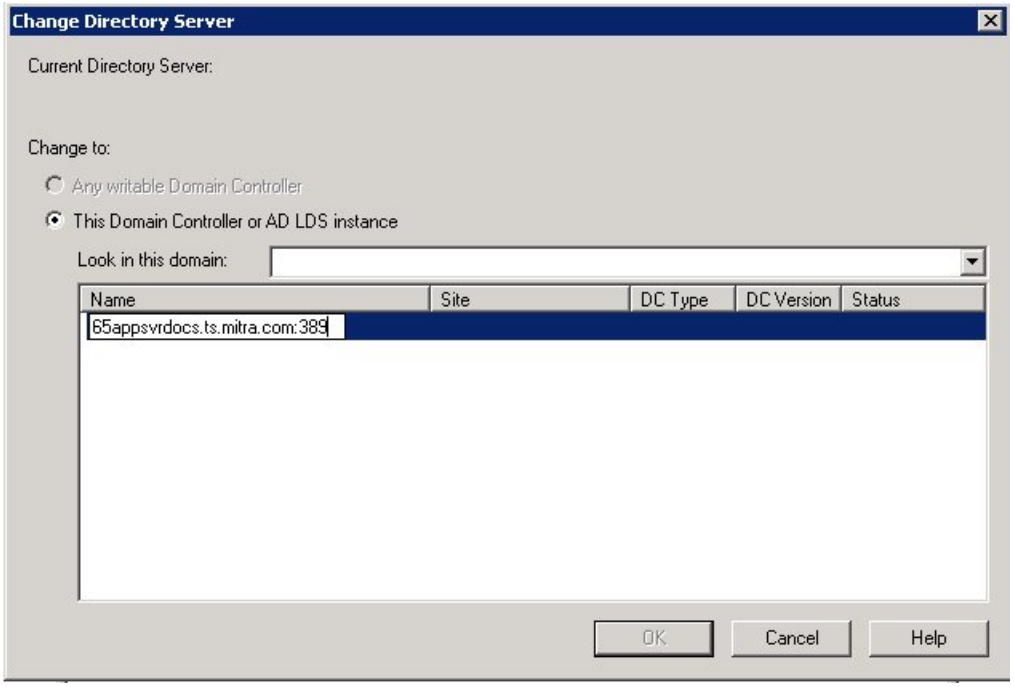
   regsvr32 schmmgmt.dll
5. Select **Start** > **Run**.
6. In the Run dialog, type **mmc**. Click **OK.**
7. Select **File** > **Add/Remove Snap-in**.
8. In the Add or Remove Snap-ins dialog, from the Available Snap-ins list, select **Active Directory Schema**



9. Click **Add**, then click **OK**.
10. Right-click **Active Directory Schema**, and select **Change Active Directory Domain Controller**



11. Click **This Domain Controller or AD LDS instance**.
12. Under Name, enter the name, the domain, and port number of the Windows 2008 replica.



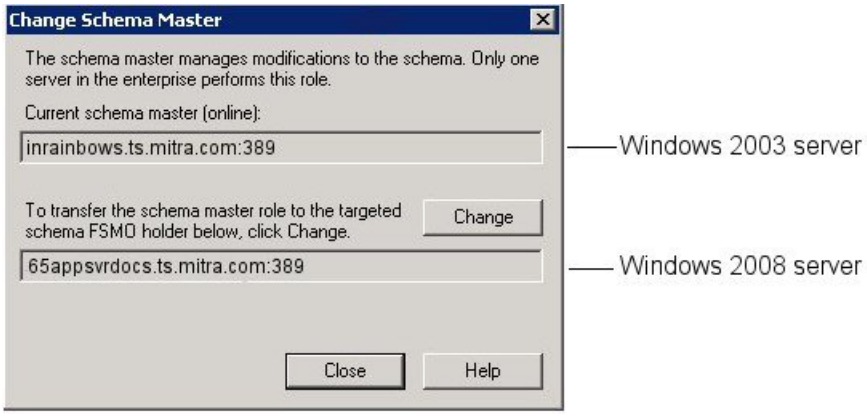
13. Click **OK**.

    A dialog is displayed informing you that the Active Directory Schema snap-in is not connected to the schema operations master.

14. Click **OK**

15. Right-click **Active Directory Schema** and select **Operations Master**.

    The Change Schema Master dialog is displayed. The current schema master (the Windows 2003 server), is shown in the Current Schema Master (online) field. The Windows 2008 server you specified in Step 12 is shown in the lower field as shown in the following illustration.



16. Click **Change**.

    A confirmation dialog is displayed, informing you that the Operations Master was successfully transferred from the Windows 2003 server to the Windows 2008 server.

17. Click **Close**.

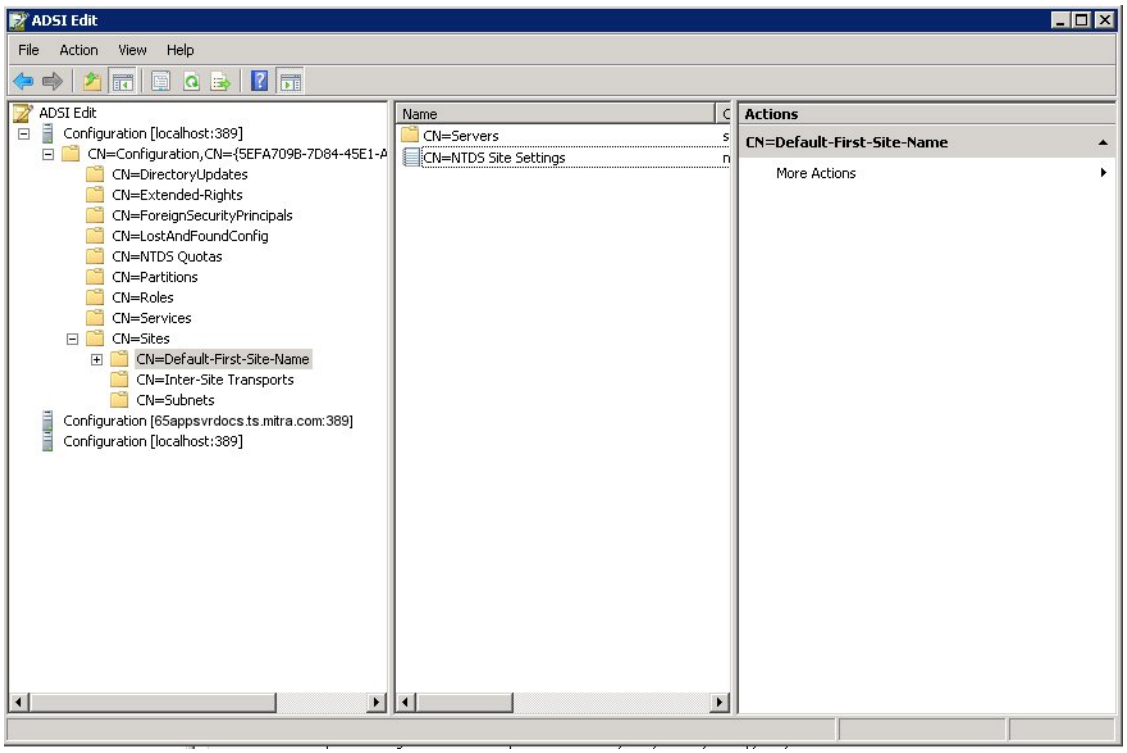
Setting up replication to repeat every 15 minutes

(Topic number: 113465)

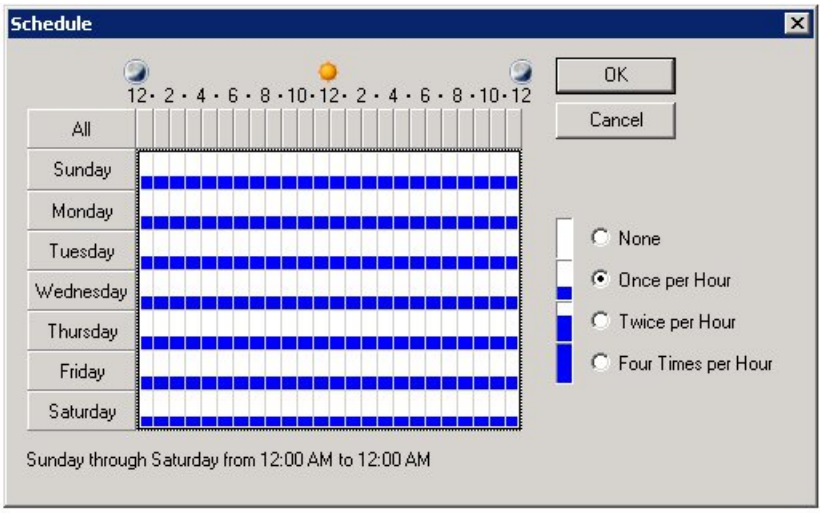
So that data remains consistent between all databases in the cluster, set up replication between AD LDS instances to occur every 15 minutes.

To set up replication to repeat every 15 minutes.

1. Log into the Windows 2008 Application Server.
2. Launch **ADSI Edit**.
3. In the left-hand pane, expand **CN=Sites**, and click **Cn=Default-First-Site-Name**.



4. In the center pane, right-click **CN=NTDS Site Settings** and select **Schedule**.
5. In the **CN=NTDS Site Settings** dialog, scroll down to the schedule attribute.
6. To set the database to replicate every hour of every day at 15 minute intervals, click **Four Times per Hour**.



7. Click **OK**.

Migrating web services plugins to the Windows 2008 Application Server

(Topic number: 120616)

When migrating from a Windows 2003 Application Server to a Windows 2008 Application Server, you must migrate the web services plugins that are used for LDAP Enterprise Authentication.

To migrate web services plugins to the Windows 2008 Application Server

1. Log into the Windows 2003 Application Server that you are using for the migration and navigate to **E:\inetpub\wwwroot\AgfaHC.User.Security.Web.Services**.
2. Open the **web.config** file.
3. Find the PluginSettings section of the file and copy it into a text editor such as Notepad and save the file.
4. Log into the Windows 2008 Application Server and navigate to **E:\inetpub\wwwroot\AgfaHC.User.Security.Web.Services**.
5. Open the **web.config** file.
6. Find the PluginSettings section of the file and replace it with the PluginSettings section from the Windows 2003 server you copied in step 3.
7. Save the modified **web.config** file.
8. Repeat steps 1-7 using the web.config files in the E:\inetpub\wwwroot\AgfaHC.User.Administration.Web.Services directory on the Windows 2003 and Windows 2008 Application Servers.

Updating the database server's map_ini table

(Topic number: 118595)

Update the ini_value in the database server's map_ini table to the name of the replica (Windows 2008) Application Server.

To update the database server's map_ini table

1. Open a SQL editor such as clui.
2. To check the current value of the map_ini table's ini_value field, type

   select ini_value from map_ini where ini_key like '%ws.authenticate.uri%'
3. If the query you ran in the previous step returns the name of the Windows 2003 Application Server used for replication, type

   update map_ini set ini_value=https://*Windows 2008 server*/AgfaHC.User.Security.Web.Services/Login.asmx where ini_section=SERVICE_TOOLS ini_key=ws.authenticate.uri

   where *Windows 2008 server* is the fully qualified domain name of the replicated Windows 2008 server.

The value of the map_ini table's ini_value field is the name of the replica (Windows 2008) Application Server.

Updating the hostname in the Agfa Security Wizard

(Topic number: 118597)

You must use the Agfa Security Wizard to update the hostname on the replicated Windows 2008 Application Server.

To update the hostname in the Agfa Security Wizard

1. Log into the Windows 2008 Application Server.
2. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
3. In the Security Wizard, select **Work with the Application Server default settings** and click **Next**.
4. In the Web Services Url Configuration dialog, in the Hostname field, enter the name of the replica Windows 2008 Application Server and click **Update**. Click **Next**.
5. In the User Management dialog, if you want to add an Administrator, select **Add Administrator** and enter a user name and password into the User Name and Password fields

   or

   If you do not want to add an Administrator, select **Do not add Administrator**.
6. Click **Next**.

7. Select either **Add Administration License** and specify a license file, or select **No Administration License**.
8. Click **Finish**.
9. Close the Agfa Security Wizard.

Verifying that the Internet station container is updated with the Windows 2008 Application Server

(Topic number: 118873)

To complete the replication, you should verify that the Internet [Default] station container in the IMPAX Client is updated with the new, replicated Windows 2008 IMPAX.

To verify that the Internet station container is updated with the Windows 2008 IMPAX,

1. Open the IMPAX Client.
2. From the **Configure** drawer menu, select **Stations**.

   or

   Or, from the List area bar, click the User ID menu and select **Station Configuration**.
3. Expand the Internet [Default] station container.
4. Verify that the newly replicated Windows 2008 IMPAX is listed.

Removing the original ADAM instance from the replication set

(Topic number: 110092)

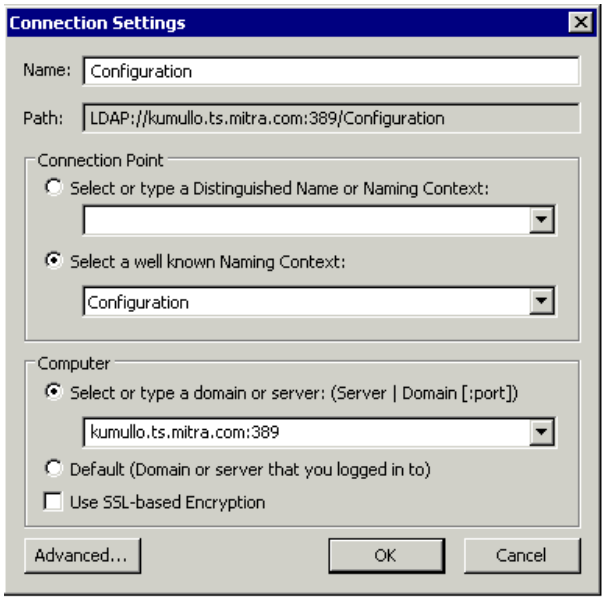
You must delete the original AgfaHealthcare entry from the replication set on the Windows 2008 Application Server.

To remove the original ADAM instance from the replication set

1. Ensure that the ADAM instance on the Windows 2003 Application Server is uninstalled and offline.
2. On the primary AD LDS instance, open the ADSI Edit snap-in.

   Note:

   If you have not set up a configuration connection to the Windows 2003 server, continue with step 3. If you have already created a configuration connection, skip ahead to step 8.
3. In the left pane of ADSI Edit, right-click **ADSI Edit** and select **Connect to**
4. In the Connection Settings dialog, in the Name field, type **Configuration**.



5. Select **Select a well known Naming Context** and from the list, select **Configuration**.
6. Type the name of the Windows 2008 server to create a connection configuration for.
7. Click **OK**.
8. In the left pane in ADSI Edit, select the **Configuration** connection.
9. Navigate to **CN=Configuration** > **CN=Sites** > **CN=Default-First-Site-Name** > **CN=Servers**.
10. Find a folder with the name of the Windows 2003 server used for replication and delete it.

Important!

Enable the Windows firewall on the Windows 2008 Application Server.

You can now re-image the Windows 2003 server with Windows Server 2008 and bring the machine into the cluster.

Adding the IMPAXServerUser and IMPAXAdminUser accounts to the ImpaxServerUser group

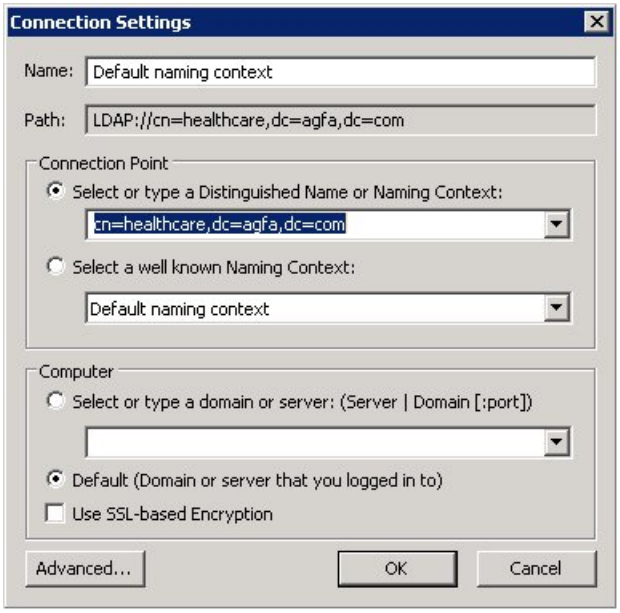
(Topic number: 119943)

After replication is complete, add the IMPAXServerUser and IMPAXAdminUser accounts to the ImpaxServerUser group on the Windows 2008Application Server.

To add the IMPAXServerUser and IMPAXAdminUser accounts to the ImpaxServerUser group

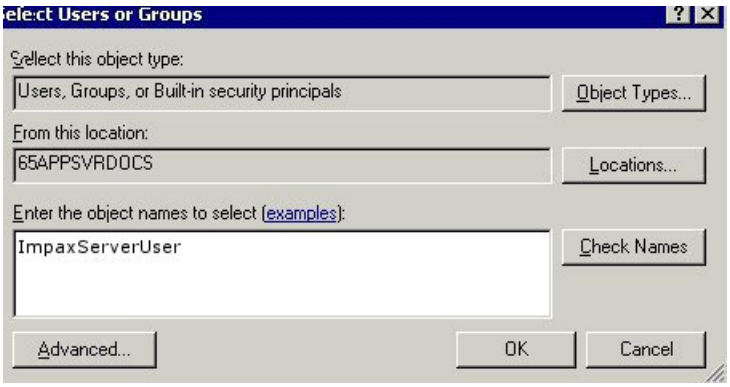
1. Log into the Application Server running Windows Server 2008.
2. Select **Start** > **Server Manager**.
3. Expand **Roles** and click **Active Directory Lightweight Directory Services**.

4. In the right-hand pane, find the **Advanced Tools** section and click **ADSI Edit**.
5. In the ADSI editor, create a connection to an AD LDS instance.
    a. Right-click **ADSI Edit** in the left-hand pane and select **Connect To**.
    b. Enter values into the Connection Settings dialog as shown and click **OK**.



6. Add the IMPAXServerUser and IMPAXAdminUser accounts to the IMPAXServerUser group.
    a. Expand **Default Naming Context** and then expand the **CN=healthcare,dc=agfa,dc=com** connection point.
    b. Select **Roles** and in the center pane, right-click the **CN=IMPAXServerUser** role and select **Properties**.
    c. In the CN=IMPAXServerUser Properties dialog, scroll down to the **member** attribute and click **Edit**.

    The Multi-valued Distinguished Names With Security Principal Editor dialog is displayed, showing the list of users associated with the member attribute.
    d. Click **Add Windows Account**.
    e. In the Select Users or Groups dialog, type **IMPAXServerUser** and click **OK**.



The account name appears in the Multi-valued Distinguished Name With Security Principal Editor dialog as a member of the IMPAXServerUser group.

f. Click **OK** twice to return to ADSI Edit.

7. Repeat step 6 to add the IMPAXAdminUser account to the IMPAXServerUser group, substituting IMPAXAdminUser for IMPAXServerUser.

Completing the migration from Windows 2003 to Windows 2008

(Topic number: 119896)

To complete the migration from Windows 2003 to Windows 2008, on the Windows 2008 Application Server, obtain an SSL certificate and assign it to the replicated AD LDS instance, then install licenses using the License Manager.

To complete the migration from Windows 2003 to Windows 2008

1. Assign a security certificate to the Windows 2008 Application Server.

   Instructions on how to create and submit a certificate request and on how to import and assign a certificate are in the following topics:

   - *Creating an SSL certificate request* (refer to page 62)
   - *Submitting a certificate request to a certificate authority* (refer to page 63)
   - *Importing an SSL certificate in the Security Wizard* (refer to page 64)
   - *Assigning an SSL certificate in the Security Wizard* (refer to page 65)

2. Request a license for the new Windows 2008 Application Server, then install and activate the license by following the instructions in the topic *Installing and Activating Licenses* (topic number 11381) in the *IMPAX 6.5.1 Application Server Knowledge Base*.

Upgrading the Application Server from a previous version

8

Important!

For AS300 Oracle and for all AS3000 (Solaris server) sites, before upgrading the Application Server, ensure that you have the correct version of Oracle 10g Client installed. For instructions on how to check the current version of the Oracle Client, see *Determining the version of the installed Oracle Client* (refer to page 130). For instructions on how to install the Oracle 10g Client, see *Installing and configuring the Oracle 10g Client for Windows* (refer to page 132).

Upgrade all Application Servers in the cluster to IMPAX 6.5.1.

Important!

All Application Servers in the same cluster must be running the same operating system. You cannot mix Application Servers running Windows Server 2003 with Application Servers running Windows Server 2008 in the same cluster.

Upgrading the Application Server on Windows Server 2003 R2 SP2

(Topic number: 131122)

When upgrading the Application Server in the cluster to IMPAX 6.5.1 and running Windows Server 2003 R2 SP2, you must migrate the ADAM database.

All Application Servers in the same cluster must be running the same operating system. You cannot mix Application Servers running Windows Server 2003 R2 SP2 with Application Servers running Windows Server 2008, in the same cluster.

Upgrading the ADAM database

(Topic number: 58664)

Unlike previous versions of the IMPAX Application Server, you do not have to manually migrate the ADAM database by running migrate.bat. Instead, the migration is performed automatically during the software upgrade.

The results of the ADAM migration are recorded in the ImpaxAdam.log file in the C:\Impax\Logs directory.

If you are upgrading a cluster to Windows Server 2008, you must replicate the ADAM database instance on a new Windows 2008 server, which uses the AD LDS database. For information on how to replicate the ADAM database on a Windows 2008 server, see *Migrating an Application Server from a Windows 2003 server to a Windows 2008 server* (refer to page 96).

Backing up the ADAM database

(Topic number: 6717)

Backing up the ADAM database at this time is important in the event that the Application Server upgrade fails.

To back up the ADAM database

1. Select **Start** > **All Programs** > **Accessories** > **System Tools** > **Backup**.
2. Select **Tools** > **Options**.
3. Switch to the **Exclude Files** tab.
4. In the list of file names, select **C:\Program Files\Microsoft ADAM** and click **Remove**. Click **OK**.
5. When the Backup or Restore Wizard is displayed, clear the **Always start in Wizard mode** checkbox and click **Advanced Mode**.
6. On the Welcome screen, click **Backup Wizard**.
7. On the Backup Wizard screen, click **Next**.
8. On the What to Backup screen, select **Backup selected files, drives, or network data**. Click **Next**.
9. On the Items to Backup screen, select the folder containing the ADAM data as well as the **World Wide Web Publishing Service** folder. Click **Next**.

   The default location for the ADAM database is C:\Program Files\Microsoft ADAM\AgfaHealthcare.
10. If backing up to a tape drive, under Backup media type, select the tape drive, and in the backup media area, click **New media**. Click **Next**.

or

If backing up to any other media type, select the location where the backup is to be saved, and type a name for the backup. Click **Next**.

11. On the Completing the Backup Wizard screen, click **Advanced**.
12. On the Type of Backup screen, select **Normal.** Click **Next**.
13. On the How to Backup screen, select **Verify data after backup and Use hardware compression if available.** Click **Next**.
14. On the Backup Options screen, select **Replace the existing backups**. Click **Next**.
15. On the When to Backup screen, select **Now**. Click **Finish**.
16. In the Backup Progress dialog, click **Close**.
17. Close the Backup Utility.

Restoring an ADAM instance

(Topic number: 11365)

Active Directory Application Mode (ADAM) data and log files should be backed up regularly to ensure the continued availability of data to applications and users in the event of a system failure. When you restore a database to an existing ADAM instance, you must stop the ADAM instance before you run the restore operation. In addition, it is recommended that you move (or delete) the existing database and log files from the ADAM instance before performing the restore operation.

To restore an ADAM instance

1. Stop the ADAM instance.
2. From the **Start** menu, select **All Programs** > **Accessories** > **System Tools** > **Backup**.
3. If the Backup or Restore Wizard is displayed, clear the **Always start in Wizard mode** checkbox, and click **Advanced Mode**.
4. In the Welcome dialog, click **Restore Wizard**.
5. In the Restore Wizard dialog, click **Next**.
6. In the What to Restore dialog, double-click the ADAM backup.
7. From the list of Items to Restore, select all files and folders in the backup and click **Next**.
8. In the Completing the Restore Wizard dialog, click **Advanced**.
9. In the Where to Restore dialog, select **Original Location** and click **Next**.
10. In the How to Restore dialog, select **Replace existing files** and click **Next**.
11. In the Advanced Restore Options dialog, select all options and click **Next**.
12. In the Completing the Restore Wizard dialog, click **Finish**.

    The ADAM database is restored from the backup.

Stopping services on the Application Servers

(Topic number: 10144)

To ensure that IMPAX Client workstations do not attempt to connect during the upgrade process, stop the Windows services on the Application Servers.

To stop services on the Application Servers

1. On an Application Server, open the Windows Administrative Tools and select **Services**.
2. In the list of services, highlight the **World Wide Web Publishing Service**.
3. Click **Stop**.
4. Repeat steps 2 and 3 for the following services:
    a. **IMPAX Distributed License Manager**
    b. **IMPAX Messaging Service**
    c. **IMPAX App Server Data Manager**
    d. **IMPAX Audit Event Log Manager**
    e. **IMPAX Dicom Object Sender**
    f. **AGFA HealthCare Service**

Uninstalling IMPAX 6.2 documentation

(Topic number: 10736)

You must uninstall the IMPAX 6.2 documentation before you can install the new IMPAX 6.5.1 documentation. Although the three IMPAX 6.2 Knowledge Bases are installed together, they must be separately uninstalled.

To uninstall the IMPAX 6.2 documentation

1. Open Control Panel.
2. Select **Add or Remove Programs**.
3. Under Currently installed programs, select **IMPAX 6.2 Documentation**.
4. Click **Change/Remove**.
5. In the Confirmation dialog, click **OK**.
6. In the Maintenance Complete dialog, click **Finish**.
7. Under Currently installed programs, select **IMPAX Application Server Knowledge Base**.
8. Click **Change/Remove**.
9. In the Confirmation dialog, click **OK**.
10. In the Maintenance Complete dialog, click **Finish**.
11. Under Currently installed programs, select **Impax Client Knowledge Base**.

12. Click **Change/Remove**.
13. In the Confirmation dialog, click **OK**.
14. In the Maintenance Complete dialog, click **Finish**.
15. Under Currently installed programs, select **IMPAX Server Knowledge Base**.
16. Click **Change/Remove**.
17. In the Confirmation dialog, click **OK**.
18. In the Maintenance Complete dialog, click **Finish**.

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

You must uninstall the IMPAX 6.3 or later documentation before you can install the new IMPAX 6.5.1 documentation.

To uninstall IMPAX 6.3 or later documentation

1. Open Control Panel.
2. In Windows 2008 Service Pack 2, select **Programs and Features**.
3. In the Programs and Features 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 Programs and Features dialog.

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

Before upgrading the IMPAX Business Services on the Application Server, uninstall the IMPAX Installation Server if an Installation Server is already installed.

To uninstall the IMPAX Installation Server

1. Open Control Panel.
2. In Windows 2008 Service Pack 2, select **Programs and Features**.
3. Select **Agfa IMPAX Installation Server *version_number*** where *version_number* is the version of the installed Installation Server.
4. Right-click and select **Uninstall**.

The Agfa IMPAX Installation Server is uninstalled.

Installing the recommended version of the Oracle Client

(Topic number: 106750)

Oracle Client is installed on all Archive Servers, Network Gateways, Curators, and Application Servers in the cluster. If not already at version 10.2.0.4, the previous version must be uninstalled before installing this version.

Important!

If you are upgrading the IMPAX Application Server from 6.5 to 6.5.1 you do not need to upgrade the Oracle Client.

Determining the version of the installed Oracle Client

(Topic number: 106578)

As part of the Oracle 10g Client installation on Windows, you first have to determine the version of the Oracle Client that is currently installed. If version 10.2.0.1.0 is installed, it must be uninstalled before you proceed with the Oracle 10g Client installation. If version 10.2.0.4.0 is installed, it must be upgraded to include the latest security patches and also ODP for .NET 2.0.

Important!

If you are upgrading the IMPAX Application Server from 6.5 to 6.5.1 you do not need to upgrade the Oracle Client.

To determine the version of the installed Oracle Client

1. Open a command prompt.
2. Type

   sqlplus -V

If the command returns `SQL*Plus: Release 10.2.0.1.0 - Production`, version 10.2.0.1 is installed and needs to be uninstalled first. For further details, see *Removing ODBC entries prior to uninstalling the Oracle Client* (refer to page 130) and *Uninstalling the previous version of Oracle Client* (refer to page 131)

If the command returns `SQL*Plus: Release 10.2.0.4.0 - Production`, version 10.2.0.4 is installed and needs to be upgraded. For further details, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 135).

Removing ODBC entries prior to uninstalling the Oracle Client

(Topic number: 119055)

Prior to removing the Oracle Client, you must remove the ODBC entries.

To remove ODBC entries prior to uninstalling the Oracle Client

1. Open the Windows Administrative Tools and select **Data Sources** (**ODBC**).
2. In the ODBC Data Source Administrator screen, select the System DSN tab.

   A list of all System DSNs is displayed, including a name and the driver associated with the DSN.
3. For each driver listed, select the associated name and click **Remove**.
4. Click **OK**.

Uninstalling the previous version of Oracle Client

(Topic number: 65367)

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 export all or part of the registry to a text file

1. To open the Registry Editor, select **Start** > **Run**.
2. In the Run dialog, type **regedit**. Click **OK**.
3. Click **File** > **Export**.
4. In the File Name field, type a name for the registry file.
5. In the Export Registry File dialog, to back up the entire registry, select **All**.
6. Click **Save**.

To retain the correct entries on the tnsnames.ora file, ensure that it is backed up prior to uninstalling Oracle Client. The tnsnames.ora file is in the **C:\oracle\product\10.2.0*client_1*\NETWORK\ADMIN** directory where *client_1* can be any arbitrary name.

If an earlier version of Oracle Client is installed on the system, uninstall that version before installing Oracle 10g Client.

To uninstall the previous version of Oracle Client

1. Select **Start** > **All Programs** > **Oracle - ohome** > **Oracle Installation Products** > **Universal Installer**.
2. Click **Deinstall Products**.
3. In the Inventory dialog on the Contents tab, select the **OraClient10_*home1*** checkbox, where *home1* can be any text.

4. Click **Remove**.
5. In the Confirmation dialog, to confirm the uninstall, click **Yes**.
6. After the uninstall is complete, to close the Universal Installer, click **Close**, then **Cancel**.
7. Open the Windows Administrative Tools and select **Services**.
8. Select the **Distributed Transaction Coordinator** service. If it started, click **Stop** to stop it.
9. From Windows Explorer, delete the ***drive_letter*:\oracle** directory.

   Drive_letter is the name of the drive where Oracle is installed.
10. From Windows Explorer, delete the **C:\Program Files\Oracle** directory.
11. Run regedit and delete the **HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE** key.
12. Restart the computer.

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

Installing and configuring the Oracle 10g Client for Windows

(Topic number: 6790)

Before installing the Oracle 10g Client, log into the server as a local administrator, and ensure that the network and TCP/IP are properly installed and configured.

Install the Oracle 10g Client software when using the Oracle Database Server, either on Solaris (AS3000) or Windows (AS300), and before connecting to an IMPAX RIS. The Oracle Client software is available for Windows 32-bit systems. It is installed on dedicated Application Servers, dedicated Curators, and dedicated AS300 Network Gateways and Archive Servers.

Note:

If installing the Application Server on the same machine as the AS300 server software, you do not have to install the Oracle 10g Client. The Oracle Server installed as part of the AS300 install contains the Client components.

If an earlier version of Oracle Client is installed on the system, uninstall that version (refer to page 131). If you have uninstalled a previous version of the Client, prior to installing the Oracle 10g Client, follow these steps.

Important!

Before installing the Oracle Client, disable virus protection software.

To install and configure the Oracle 10g Client for Windows

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

   Cygwin is automatically installed before Oracle is.
3. At the `Install Oracle "client" or "server"?` prompt, type **client**.
4. At the `Hostname of the Oracle server [] ?` prompt, type the correct host name of the IMPAX Database Server.
5. At the `What machine is the repository host? [localhost]` prompt, if it is the localhost, press **Enter**. Otherwise, specify the appropriate IP address.
6. At the `Where is the software repository?` prompt, if installing from the DVD drive on F, press **Enter**. Otherwise, type the DVD drive or software repository directory.
7. At the `Where is the temporary work directory? [ C:\cygwin\temp] ?` prompt, click **Enter** to accept the default location. Otherwise, type the directory to use.

   A series of messages appears as Oracle is installed and configured.
8. After the `Oracle installation complete` message appears, restart the server.

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

Setting up a connection to the Oracle database

(Topic number: 46341)

The Oracle 10g Client (version 10.2.0.4) software installs the drivers and programs required to communicate with the Oracle Server. Ensure that the network and TCP/IP are properly installed and configured.

To set up a connection to the Oracle database

1. If the Net Configuration Assistant is not open, select **Start** > **All Programs** > **Oracle - ohome** > **Configuration and Migration Tools** > **Net Configuration Assistant**.
2. In the Oracle Net Configuration Assistant Welcome dialog, select **Local Net Service Name configuration** and click **Next**.
3. If the Naming Methods Configuration dialog appears, select **Local Naming**. Click **Next**.
4. In the Net Service Name Configuration screen, select **Add**. Click **Next**.
5. In the Service Name field, type **MVF**. Click **Next**.
6. From the list of protocols, select **TCP**. Click **Next**.
7. In the TCP/IP dialog, type the hostname of the Oracle server.
8. Accept the default port number (1521). Click **Next**.
9. Select **Yes, perform a test**. Click **Next**.

   The first time the test runs, you see an error message. Ignore the error.
10. Click **Change Login**.
11. In the Username field, type **mvf**, and type the password for the mvf user.
12. Click **OK**.

The test is performed again. The connection should be successful.

13. Click **Next**.
14. In the Net Service Name field, ensure that **MVF.world** appears. Click **Next**.
15. If you do not want to add a net service name for RIS, select **No**. Click **Next**.

    or

    To add a net service name for RIS, at the prompt to configure another net service name, select **Yes**. Click **Next**. Then repeat all previous steps using a different service name (for example, qprod), as well as a different host name, login, and net service name (for example QPROD.WORLD).
16. In the Net Service Name Configuration Complete dialog, click **Next**.
17. In the Naming Methods Configuration Complete dialog, click **Next**.
18. To close the Net Configuration Assistant dialog, click **Finish**.

Reconfiguring ODBC data source names

(Topic number: 67665)

A Data Source Name (DSN) is the name used by Open Database Connectivity (ODBC) to refer to the system required to access data. The name is used by Internet Information Services (IIS) for a connection to an ODBC data source, such as the Oracle database.

Before upgrading Oracle Server (and changing the Oracle home) on the Database Server, the existing mvf and mvf_ora DSNs were removed from all Windows-based servers (but not on the IMPAX Client stations) and may now need to be reconfigured.

To reconfigure ODBC data source names

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

   where *Oracle_instance_name* is the name typed when *Installing and configuring the Oracle 10g Client for Windows* (refer to page 132).
6. Click **Finish**.
7. In the Data Source Name field, type **mvf**.
8. Type a description, if needed.
9. In the TNS Service Name field, type **MVF.world**.
10. In the User Name field, type **mvf**.

    The user ID must be lowercase.
11. To save the changes and close the dialog, click **OK**.
12. To save the new sources and exit the ODBC Data Source Administrator dialog, click **OK**.

13. If reconfiguring the Application Server, repeat the previous steps for the **mvf_ora** DSN as well.

Upgrading to the 10.2.0.4 version of the Oracle Client for Windows

(Topic number: 106600)

Important!

If you are upgrading the IMPAX Application Server from 6.5 to 6.5.1, you do not need to upgrade the Oracle Client.

If the Oracle Client version 10.2.0.4 is installed on your system, upgrade it to include the latest security patches and also install ODP for .NET 2.0. To do so, you must be logged into Windows as an administrator-level user.

To upgrade to the 10.2.0.4 version of the Oracle Client for Windows

1. Insert the Oracle on Windows 32-bit DVD.
2. Open a command prompt.
3. Change to the **C:\mvf-mig6\bin** directory.
4. Type **bash upgrade-oracle *location_of_DVD_drive_or_Oracle_software_repository***

   For example, **bash upgrade-oracle d:**
5. When you see the message `Ready to upgrade Oracle using repository Oracle software location. Do you want to proceed? [y/n]`, verify that the oracle software location is correct. If the location is correct, type **y** and press **Enter**.

The Oracle Client is upgraded.

Upgrading the IMPAX Application Server software to 6.5.1

(Topic number: 9863)

Note:

This installation does not overwrite the existing ADAM database.

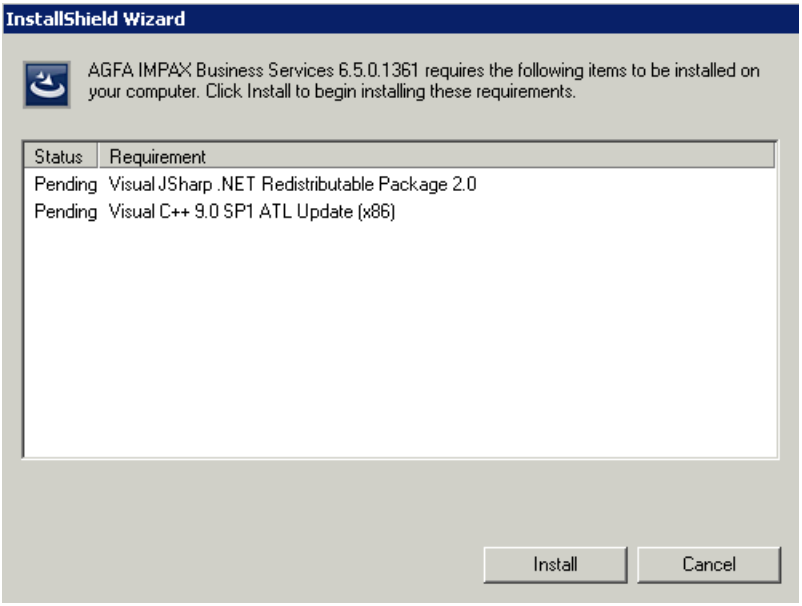
To upgrade the IMPAX Application Server software to 6.5.1

1. Insert the IMPAX Business Services CD.
2. Navigate to the CD ROM drive, which contains the Business Services software.
3. Run **AGFA IMPAX Business Services Setup.exe**.

   The following packages are installed on the Application Server prior to the upgrade.
   - 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, they are installed when you click **Install**. If any of these packages do not appear in the list, those packages are already installed on the machine.



4. Click **Install**.
5. On the Welcome screen, click **Next**.
6. On the license agreement screen, select **I accept the terms in the license agreement**. Click **Next**.
7. On the Web Services Installation Folder screen, click **Change**.
8. Set the path to the **wwwroot** directory so that it matches the pre-upgrade installation location. Click **OK**.

   For example, set the path to J:\wwwroot rather than C:\inetpub\wwwroot.
9. Click **Next**.
10. On the Setup Type screen, select **Custom**. Click **Next**.
11. If you have an IMPAX RIS to connect to, click **RIS Web Services** and select **This feature will be installed on local hard drive**.
12. If you are using SmartCard authentication, verify that **NHS SmartCard Web Services** is selected. If it is not selected, select it. Select **This feature will be installed on local hard drive**.
13. Click **Next**.
14. Click **Install**.
15. On the InstallShield Wizard Completed screen, select **Launch IMPAX Business Services Configuration tool**. Click **Finish**.
16. When the message `Previous configuration found from version 6.X.X...` appears, click **Yes**. This message is not displayed when upgrading from IMPAX 6.5 to IMPAX 6.5.1.

17. In the Configuration Tool, click **Apply**.
18. To close the Configuration Tool, click **OK**.

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 128). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 143).

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* (refer to page 88)

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 147)) or on a separate, dedicated Windows-based server.

Note:

If your site has a large number of IMPAX Clients, or they are regularly updated, using an Application Server as an Installation Server may affect the performance of Clients connected to that Application Server. This is because the Clients all check for a new version every 30 minutes and, although staggered, performance issues have been reported when many Clients are downloading the new IMPAX Client software.

Therefore, we recommend:

- Using a third-party software distribution application (for example, Microsoft SMS or Altiris) to avoid saturation of the Application Server. Consult your regional Agfa representative for options.
- Placing the Installation Server on a dedicated server.

If you choose to install the IMPAX Installation Server package on a dedicated server, use the Web Server Certificate Wizard to create a certificate request to submit to a trusted certificate authority, and install the certificate. You must install the SSL certificate on the dedicated server before installing the IMPAX Installation Server package.

The Installation Server Setup package contains:

- The installers (or links) for the IMPAX Client prerequisites:
  - .NET Framework 3.5 SP1
  - Visual C++ 9.0 SP1
  - DirectX
- The IMPAX Client Installer
- A web page with links to:
  - IMPAX Client system requirements

- IMPAX Client installation instructions (available in 19 languages)
- Links to the IMPAX Client Installer
- Links to the individual perquisites

Running the IMPAX Installation Server package

(Topic number: 7758)

CAUTION!

Do not install the IMPAX Installation Server on a standalone IMPAX workstation (a workstation running the AS300, Application Server, and Client software).

The following explains how to install the IMPAX Installation Server to use as a distribution tool for Client installations and updates.

To run the IMPAX Installation Server package

1. From the IMPAX Client CD or a network location, run **IMPAXInstallationServerSetup.exe**.

   A Preparing to install message appears.
2. On the Welcome to the InstallShield Wizard for IMPAX Installation Server screen, click **Next**.
3. To install the application into C:\Inetpub\wwwroot\ClientInstaller, 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**.
4. On the Ready to Install the Program screen, click **Install**.

   The first installer runs.
5. On the Installation Wizard Completed screen, click **Finish**.

   Another installer starts. (It may start before the first one finishes.) The second one opens a command prompt that creates a manifest file.
6. On the second Installation Wizard Completed screen, click **Finish**.

   In the folder where the application was installed, several subfolders appear, including:
   - redist—contains the .NET Framework installers.
   - installer—contains the ImpaxClientSetup.exe, the IMPAX Client installation software.

For the updater service, which allows all installed Clients to receive automatic updates, public and private key pairs are installed in C:\Program Files\Agfa\IMPAX Client. Refer to "Configuring automatic Client updates" in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

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 Application Server, 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**.

Upgrading additional Application Servers in the cluster

(Topic number: 11210)

Perform the following tasks on each additional Application Server in the cluster.

To upgrade additional Application Servers in the cluster.

1. Uninstall the IMPAX 6.2, 6.3, or 6.4 documentation.
2. Upgrade the IMPAX Application Server software (refer to page 135).
3. Install the IMPAX 6.5.1 Documentation (refer to page 145).
4. Verify the installation.

Upgrading the Application Server on Windows Server 2008 SP2

(Topic number: 131128)

When upgrading the Application Server in the cluster to IMPAX 6.5.1 and running Windows Server 2008 SP2, you must migrate the AD LDS database.

All Application Servers in the same cluster must be running the same operating system. You cannot mix Application Servers running Windows Server 2008 SP2 with Application Servers running Windows Server 2003 R2 SP2, in the same cluster.

Upgrading the AD LDS database from IMPAX 6.5 to IMPAX 6.5.1

(Topic number: 130063)

Unlike previous versions of the IMPAX Application Server, the AD LDS database must be migrated when upgrading from IMPAX 6.5 to 6.5.1. The migration is performed automatically during the software upgrade.

The results of the AD LDS migration are recorded in the ImpaxAdam.log file in the C:\Impax\Logs directory.

If you are upgrading a cluster to Windows Server 2008, you must replicate the ADAM database instance on a new Windows 2008 server, which uses the AD LDS database. For information on how to replicate the ADAM database on a Windows 2008 server, see *Migrating an Application Server from a Windows 2003 server to a Windows 2008 server* (refer to page 96).

Creating a one-time backup of AD LDS

(Topic number: 113662)

On Application Servers running Windows Server 2008, all IMPAX user information is stored in the AD LDS database.

To create a one-time backup of AD LDS

1. To open an elevated command prompt, click **Start**, right-click **Command Prompt** and select **Run as administrator**.
2. At the command prompt, type

   dsdbutil
3. At the dsdbutil prompt, type

   activate instance AgfaHealthcare
4. At the dsdbutil prompt, type

   ifm
5. At the ifm prompt, type

   create full *location*

   where *location* is the path to the folder where you want the installation media to be created. You can save the installation media to a network shared folder or to any other type of removable media.

   Example:

   ifm: create full C:\Backup\AgfaHealthcare
6. At the ifm prompt, type

   quit

   At the dsdbutil prompt, type

   quit

The AD LDS instance is backed up.

Restoring an AD LDS instance

(Topic number: 115214)

Active Directory Lightweight Directory Services (AD LDS) data and log files must be backed up regularly to ensure the continued availability of data to applications and users in the event of a system failure. When you restore a database to an existing AD LDS instance, you must stop the AD LDS instance before running the restore operation. In addition, we recommend that you move (or delete) the existing database and log files from the AD LDS instance before performing the restore operation.

To restore an AD LDS instance

1. Stop the **AgfaHealthcare** service.
2. Delete the files in the **"%ProgramFiles%\Microsoft ADAM\AgfaHealthcare\data"** folder.
3. At a command prompt, type

   xcopy /os <location>\adamntds.dit "%ProgramFiles%\Microsoft ADAM\AgfaHealthcare\data\adamntds.dit"

   where <location> is the path to the folder where the backup file was created.

   For example:

   xcopy /os C:\Backup\AgfaHealthcare\adamntds.dit "%ProgramFiles%\Microsoft ADAM\Agfa Healthcare\data\adamntds.dit"
4. Start the **AgfaHealthcare** service.
5. Restart Windows Server.

For more information about restoring an AD LDS instance, refer to http://technet.microsoft.com/en-us/library/cc770886(WS.10).aspx.

Stopping services on the Application Servers

(Topic number: 10144)

To ensure that IMPAX Client workstations do not attempt to connect during the upgrade process, stop the Windows services on the Application Servers.

To stop services on the Application Servers

1. On an Application Server, open the Windows Administrative Tools and select **Services**.
2. In the list of services, highlight the **World Wide Web Publishing Service**.
3. Click **Stop**.
4. Repeat steps 2 and 3 for the following services:
   a. **IMPAX Distributed License Manager**
   b. **IMPAX Messaging Service**
   c. **IMPAX App Server Data Manager**
   d. **IMPAX Audit Event Log Manager**
   e. **IMPAX Dicom Object Sender**
   f. **AGFA HealthCare Service**

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

You must uninstall the IMPAX 6.3 or later documentation before you can install the new IMPAX 6.5.1 documentation.

To uninstall IMPAX 6.3 or later documentation

1. Open Control Panel.
2. In Windows 2008 Service Pack 2, select **Programs and Features**.
3. In the Programs and Features 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 Programs and Features dialog.

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

Before upgrading the IMPAX Business Services on the Application Server, uninstall the IMPAX Installation Server if an Installation Server is already installed.

To uninstall the IMPAX Installation Server

1. Open Control Panel.
2. In Windows 2008 Service Pack 2, select **Programs and Features**.
3. Select **Agfa IMPAX Installation Server *version_number*** where *version_number* is the version of the installed Installation Server.
4. Right-click and select **Uninstall**.

The Agfa IMPAX Installation Server is uninstalled.

Upgrading the IMPAX Application Server software to 6.5.1

(Topic number: 126080)

Note:

This installation does not overwrite the existing ADAM database.

To upgrade the IMPAX Application Server software to 6.5.1

1. Insert the IMPAX Business Services CD.
2. Navigate to the CD ROM drive, which contains the Business Services software.
3. Click **Install**.
4. On the Welcome screen, click **Next**.

5. On the license agreement screen, select **I accept the terms in the license agreement**. Click **Next**.
6. On the Web Services Installation Folder screen, click **Change**.
7. Set the path to the **wwwroot** directory so that it matches the pre-upgrade installation location. Click **OK**.

   For example, set the path to J:\wwwroot rather than C:\inetpub\wwwroot.
8. Click **Next**.
9. On the Setup Type screen, select **Custom**. Click **Next**.
10. If you have an IMPAX RIS to connect to, click **RIS Web Services** and select **This feature will be installed on local hard drive**.
11. If you are using SmartCard authentication, verify that **NHS SmartCard Web Services** is selected. If it is not selected, select it. Select **This feature will be installed on local hard drive**.
12. Click **Next**.
13. Click **Install**.
14. On the InstallShield Wizard Completed screen, select **Launch IMPAX Business Services Configuration tool**. Click **Finish**.
15. In the Configuration Tool, click **Apply**.
16. To close the Configuration Tool, click **OK**.

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 128). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 143).

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* (refer to page 88)

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 147)) or on a separate, dedicated Windows-based server.

Note:

If your site has a large number of IMPAX Clients, or they are regularly updated, using an Application Server as an Installation Server may affect the performance of Clients connected to that Application Server. This is because the Clients all check for a new version every 30 minutes and, although staggered, performance issues have been reported when many Clients are downloading the new IMPAX Client software.

Therefore, we recommend:

- Using a third-party software distribution application (for example, Microsoft SMS or Altiris) to avoid saturation of the Application Server. Consult your regional Agfa representative for options.

- Placing the Installation Server on a dedicated server.

If you choose to install the IMPAX Installation Server package on a dedicated server, use the Web Server Certificate Wizard to create a certificate request to submit to a trusted certificate authority, and install the certificate. You must install the SSL certificate on the dedicated server before installing the IMPAX Installation Server package.

The Installation Server Setup package contains:

- The installers (or links) for the IMPAX Client prerequisites:
  - .NET Framework 3.5 SP1
  - Visual C++ 9.0 SP1
  - DirectX
- The IMPAX Client Installer
- A web page with links to:
  - IMPAX Client system requirements
  - IMPAX Client installation instructions (available in 19 languages)
  - Links to the IMPAX Client Installer
  - Links to the individual perquisites

Running the IMPAX Installation Server package

(Topic number: 7758)

CAUTION!

Do not install the IMPAX Installation Server on a standalone IMPAX workstation (a workstation running the AS300, Application Server, and Client software).

The following explains how to install the IMPAX Installation Server to use as a distribution tool for Client installations and updates.

To run the IMPAX Installation Server package

1. From the IMPAX Client CD or a network location, run **IMPAXInstallationServerSetup.exe**.

   A Preparing to install message appears.
2. On the Welcome to the InstallShield Wizard for IMPAX Installation Server screen, click **Next**.
3. To install the application into C:\Inetpub\wwwroot\ClientInstaller, 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**.

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

   The first installer runs.

5. On the Installation Wizard Completed screen, click **Finish**.

   Another installer starts. (It may start before the first one finishes.) The second one opens a command prompt that creates a manifest file.

6. On the second Installation Wizard Completed screen, click **Finish**.

   In the folder where the application was installed, several subfolders appear, including:

   - redist—contains the .NET Framework installers.
   - installer—contains the ImpaxClientSetup.exe, the IMPAX Client installation software.

For the updater service, which allows all installed Clients to receive automatic updates, public and private key pairs are installed in C:\Program Files\Agfa\IMPAX Client. Refer to "Configuring automatic Client updates" in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

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 Application Server, 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**.

Upgrading additional Application Servers in the cluster

(Topic number: 11210)

Perform the following tasks on each additional Application Server in the cluster.

To upgrade additional Application Servers in the cluster.

1. Uninstall the IMPAX 6.2, 6.3, or 6.4 documentation.
2. Upgrade the IMPAX Application Server software (refer to page 135).
3. Install the IMPAX 6.5.1 Documentation (refer to page 145).
4. Verify the installation.

Uninstalling components

A

The following information may be required at your site.

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 2003, select **Add or Remove Programs**. Under Windows 2008, select **Programs and Features**.
2. On Windows 2003 servers, under Currently installed programs, select any instance of **Agfa IMPAX Business Services 6.5.1** and click **Remove**.

   or

   On Windows 2008 servers, select any instance of **Agfa IMPAX Business Services 6.5.1** and click **Uninstall**.
3. On Windows 2003 servers, select **ADAM Instance AgfaHealthcare** and click **Remove**.

   or

   On Windows 2008 servers, 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 2003, select **Add or Remove Programs**. 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.

Installing an IMPAX AS300 single-server

B

A number of tasks are required to set up an IMPAX AS300 single-server. An overview is provided here with references to the appropriate publications for detailed instructions.

Note:

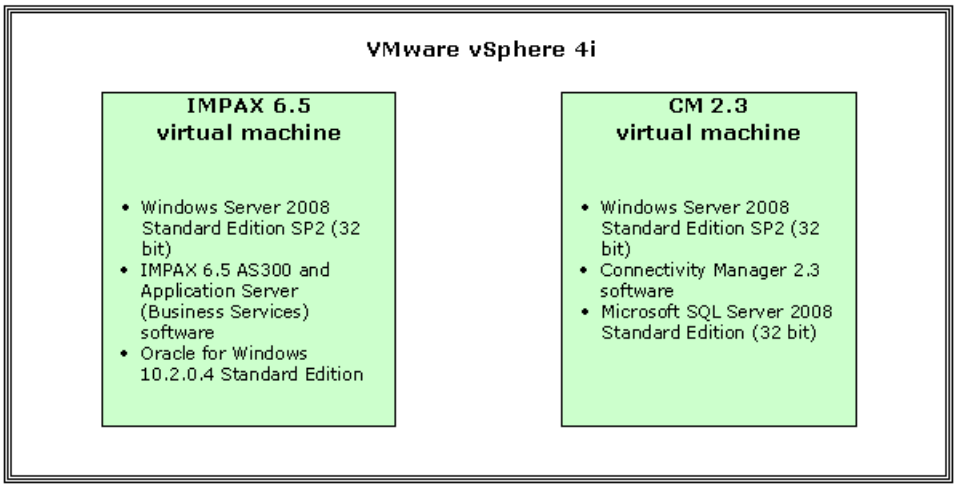
To upgrade an AS300 single-server from IMPAX 6.3 or earlier, a re-install of IMPAX and Connectivity Manager is necessary. To upgrade from IMPAX 6.4 or later, or for assistance in upgrading from IMPAX 6.3 or earlier, contact Agfa Professional Services.

What is the IMPAX single-server configuration?

(Topic number: 15477)

In an IMPAX single-server configuration, the IMPAX AS300 single-host server, IMPAX Application Server, and Connectivity Manager software are all installed on the same computer using VMware. This configuration is useful for smaller sites with a limited budget.

The VMware vSphere 4i virtualization layer is installed directly on the hardware internal RAID, and hosts the guest operating systems. The IMPAX 6.5 virtual machine runs side-by-side the Connectivity Manager 2.3 virtual machine as follows:



Note:

The IMPAX single-server platform does not allow for a client installation on top of the server configuration; however, an IMPAX standalone station does combine server and client configurations. For more information, see the *IMPAX 6.5.1 Standalone Installation and Configuration Guide*.

What is VMware ESX 4i?

(Topic number: 67081)

VMware ESX 4i is virtualization software that can host other operating systems in such a way that each operating system behaves as if it were installed on a self-contained computer with its own set of programs and hardware resources. Using VMware ESX 4i, 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

Connectivity Manager overview

(Topic number: 31597)

Connectivity Manager is one component of an integrated radiology enterprise system, and is a tool for the integration of your clinical environment.

One of the major requirements of integrating a hospital is connecting the hospital's information systems, PACS, and modalities. Connectivity Manager is a middleware component in the integration

between hospital information systems and other hospital imaging departments. Connectivity Manager also provides connectivity to modalities and the PACS.

Connectivity Manager functionality includes:

- Accepting demographic and order information from information systems (HIS/RIS/CIS) and providing the information to other systems and devices
- Performing HIS verification
- Protecting data integrity, and providing for enhanced armoring and security
- Accepting reports from external reporting systems embedded in HL7 ORU messages and storing the reports on IMPAX
- Delivering reports to external applications such as IMPAX and WEB1000
- Providing support for IMPAX EPR, for TalkStation, and for multi-site configurations
- Trimming the Connectivity Manager cache (Agfa Connectivity Autopilot)
- Providing support for the IHE Scheduled Workflow and Patient Information Reconciliation Integration profiles in combination with IMPAX 6.0
- Providing support for specific Asian (CJK) and European languages
- Authenticating users using LDAP, MVF (IMPAX 5.2 only), or Windows Domain
- Allowing connectivity between TalkStation and CHCS
- Accepting HL7 radiology procedure master files
- Providing support for DICOM SR as a report storage format
- Accommodating VA supported workflows
- Allowing improved clinical data browsing

Installing an AS300 single-server: Workflow

(Topic number: 67076)

Before proceeding with the IMPAX AS300 single-server installation, ensure that you have the correct product installation locations or CDs for VMware, Connectivity Manager 2.3, AS300 single-host server, and Application Server.

To install an AS300 single-server

1. Install ESX 4i Freeware virtualization platform from https://www.vmware.com/products/esxi/.

   For more details, refer to the *VMware ESX Server 3.x and VirtualCenter 2.x Service Manual* and to the manufacturer's installation documentation, or contact Agfa Professional services.

The ESX 4i Virtualization infrastructure is installed directly on the hardware internal RAID and hosts the operating systems of the applications. On the ESX 4i platform, an AS300 single-host and Application Server virtual machine runs side-by-side a Connectivity Manager virtual machine.

2. Install Connectivity Manager 2.3.

   Refer to the *Connectivity Manager 2.3 Installation and Configuration Guide* for detailed installation instructions.

3. Define the Connectivity Manager 2.3 settings without interfering with the IMPAX installations to come.

   Refer to the *Connectivity Manager 2.3 Installation and Configuration Guide* for detailed configuration instructions.

4. Install the AS300 single-host server.

   Detailed installation instructions are provided in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

5. Install and configure the Application Server.

   Consult *Installing IMPAX Business Services* (refer to page 46) and *Configuring the Application Server* (refer to page 53) for detailed installation and configuration instructions.

Installing Application Servers in a load-balanced environment

C

To set up Application Servers in a load-balanced environment, install either Windows Server 2003 or Windows Server 2008 on all Application Servers in the cluster, then configure one Application Server as the primary server, and configure the remaining servers as secondary.

Installing load-balanced Application Servers: Prerequisites

(Topic number: 119727)

Before setting up load balancing, on each Application Server, you must perform the following tasks.

To install load-balanced Application Servers: Prerequisites

1. Install and configure the Windows operating system.

   Note:

   All Application Servers in the cluster must run the same operating system—either Windows Server 2003 or Windows Server 2008.

   Instructions on how to install and configure Windows 2003 are in the section *Installing and configuring Windows Server 2003 SP2* (refer to page 23). Instructions on how to install and

configure Windows 2008 are in the section *Installing and configuring Windows Server 2008* (refer to page 32).

2. Configure the connection between the Application Server and the Database Server.

In addition to the instructions provided in this guide, the following *IMPAX 6.5 Application Server Knowledge Base* topics have information relevant to setting up a load-balanced environment.

Title	Topic number
Load balancing: Distributing data requests over multiple Application Servers	11348
Load balancing: Concepts	11351
Installing a load balancer in the cluster	11350
Configuring the IMPAX Client Installer for a load balancer	11349
Copying an SSL certificate to another Application Server	11427

Setting up the primary Application Server

(Topic number: 119717)

Perform these tasks on the server you want to designate as the primary Application Server.

To set up the primary Application Server

1. Install the IMPAX Business Services by following the instructions in *Installing IMPAX Business Services* (refer to page 46).
2. Configure the Application Server by following the instructions in *Configuring the Application Server* (refer to page 53).
3. Request local and enterprise SSL certificates by following the instructions in *Creating an SSL certificate request* (refer to page 62). On the web server, select **Allow certificate to be installed on multiple machines (exportable)**.
4. Assign the enterprise SSL certificate to IIS on the web server by following the instructions in *Assigning an enterprise SSL certificate to IIS* (refer to page 160).
5. Assign the local SSL certificate to ADAM (Windows 2003) or to AD LDS (Windows 2008) on the primary Application Server by following the instructions in *Assigning a local SSL certificate to ADAM/AD LDS* (refer to page 160).
6. Change the host name of the primary Application Server by following the instructions in the *Updating the primary Application Server's hostname* (refer to page 161)
7. Configure the enterprise URL by following the instructions in *Configuring the enterprise URL on the Application Server* (refer to page 162).
8. Edit the login message by following the instructions in *Editing the login message in the primary Application Server's web.config file* (refer to page 162).

9. Export the enterprise SSL certificate by following the instructions in *Copying an SSL certificate to another Application Server* (refer to page 163).
10. Configure the AgfaService user to start the AgfaHealthcare service.

Setting up one or more secondary Application Servers

(Topic number: 119573)

Perform these tasks on every other Application Server in the cluster.

To set up one or more secondary Application Servers

1. Install the IMPAX Business Services software by following the instructions in *Installing the IMPAX Business Services* (refer to page 49).
2. Copy the SSL Certificate from the primary Application Server to the secondary Application Server by following the instructions in *Copying an SSL certificate to another Application Server* (refer to page 163).
3. Configure the Application Server by following the instructions in *Configuring the Application Server* (refer to page 53).
4. Request a local SSL certificate by following the instructions in the section *Creating an SSL certificate request* (refer to page 62) This certificate is for server communication only. Therefore, it can be either a PDC certificate or an EnterpriseCA, which typically last longer.
5. Assign the enterprise SSL certificate to IIS by following the instructions in *Assigning an enterprise SSL certificate to IIS* (refer to page 160).
6. Update the hostname on the secondary server by following the instructions in *Updating the secondary Application Server's hostname* (refer to page 161).
7. Configure the enterprise URL by following the instructions in *Configuring the enterprise URL on the Application Server* (refer to page 162).
8. If applicable (using Windows only), ignore the error about not connecting to Oracle. The connection works once the server is on the domain.
9. Disable the IMPAX IPSec policy.

   This allows the system to join a domain.
10. Connect to the domain.
11. Re-enable the IMPAX IPSec policy.
12. Stop IIS and stop all IMPAX and ADAM (Windows 2003) or AD LDS (Windows 2008) services.

    For example, net stop w3svc.
13. Remove **ADAM Instance AgfaHealthcare** (Windows Server 2003) or **AD LDS Instance AgfaHealthcare** (Windows Server 2008).

14. If the Application Server cluster is running Windows 2003, create a replica of the primary Application Server's ADAM database by following the instructions in the section *Replicating ADAM* (refer to page 92).

    or

    If the Application Server cluster is running Windows 2008 and all servers in the cluster belong to the same domain, create a replica of the primary Application Server's AD LDS database by following the instructions in the section *Replicating AD LDS* (refer to page 93).

    or

    If the Application Server cluster is running Windows 2008 and all servers in the cluster belong to a workgroup, create a replica of the primary Application Server's AD LDS database by following the instructions in the section *Replicating the AD LDS database between two Windows 2008 servers in a workgroup* (refer to page 167).

15. Restart the IMPAX and IIS services.
16. Launch the Security wizard.
17. Assign the local SSL certificate to ADAM (Windows 2003) or AD LDS (Windows 2008) by following the instructions in the section *Assigning a local SSL certificate to ADAM/AD LDS* (refer to page 160).
18. Restart the IMPAX and w3svc services.
19. To confirm connectivity, open an Internet Explorer window and type:

    https://<SecondaryApplicationServerName/agfahc.user.security.web.services/login.asmx

20. Log in as a user on the primary ADAM/AD LDS instance.
21. Edit the login message in the E:\wwwroot\AgfaHC.User.Security.Web.Services\web.config file by following the instructions in the section *Editing the login message in the primary Application Server's web.config file* (refer to page 162).
22. Log into the web server from an IMPAX Client and observe the message in the login GUI. Ensure that the load balancer is routing to both the primary Application Server and the secondary Application Server. This may take a few attempts.
23. Install impaxinstallationserver.exe on each Application Server in the E:\wwwroot\ClientInstaller directory.
24. Configure the ClientInstaller. Create a manifest file for the Clients by running the following commands:

    E:\wwwroot\ClientInstaller>CreateManifest.exe -f

    E:\wwwroot\ClientInstaller -v <Client version> -m <*Enterprise Application Server fully qualified domain name*> -u http

    where *<Enterprise Application Server fully qualified domain name>* is the enterprise URL and not the local hostname of the Application Server.

25. On all Application Servers, update the hosts file. Create an entry for the Enterprise URL server that points to the local IP address, not the load balancer IP address. This allows the Healthcheck URL to work.

Assigning certificates to services using the Security Wizard

(Topic number: 119515)

To set up load-balanced Application Servers, you need two certificates. One certificate is required to support the local ADAM/AD LDS service, and a second certificate is required to support the load-balanced VIP name.

Assign the enterprise SSL certificate to IIS, then assign the local SSL certificate to the ADAM (Windows 2003) or AD LDS (Windows 2008) service.

Assigning an enterprise SSL certificate to IIS

(Topic number: 119482)

On the web server, assign the enterprise SSL certificate to IIS.

To assign an enterprise SSL certificate to IIS

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
2. In the Security Wizard, select **Work with SSL certificates**. Click **Next**.
3. Select **Assign an existing certificate to services**. Click **Next**.
4. From the list of certificates, select the enterprise certificate and click **Next**.
5. In the Available Services dialog, clear **ADAM: AgfaHealthcare** and ensure that **Internet Information Services** is selected.
6. Click **Finish.**
7. On the screen displaying the message `Successfully applied certificate to services`, click **OK**.

The enterprise certificate is applied to IIS.

Assigning a local SSL certificate to ADAM/AD LDS

(Topic number: 119484)

On the primary Application Server, assign the local SSL certificate to the ADAM (Windows 2003) or AD LDS (Windows 2008) service.

To assign the local SSL certificate to ADAM/AD LDS

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
2. In the Security Wizard, select **Work with SSL certificates**. Click **Next**.
3. Select **Assign an existing certificate to services**. Click **Next**.

4. From the list of certificates, select the local certificate and click **Next**.
5. In the Available Services dialog, clear **Internet Information Services** and ensure that **ADAM: AgfaHealthcare** is selected.
6. Click **Finish.**
7. On the screen displaying the message `Successfully applied certificate to services`, click **OK**.

The local certificate is applied to the ADAM (Windows 2003) or AD LDS (Windows 2008) service.

Updating the primary Application Server's hostname

(Topic number: 120299)

Use the Agfa Security Wizard to update the hostname on each server in a load-balance cluster.

To update the primary Application Server's hostname

1. Log into primary Application Server.
2. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
3. In the Security Wizard, select **Work with the Application Server default settings** and click **Next**.
4. On the Web Services Url Configuration screen, in the Hostname field, enter the enterprise URL and click **Update**. Click **Next**.
5. On the User Management screen, select **Add Administrator** and enter a user name and password into the User Name and Password fields.
6. On the screen displaying the message `Successfully created user in the Administrators role`, click **OK**.
7. Click **Next**.
8. On the User Management screen, accept the default **Add Administration License** and click the box to the right of the License File field.
9. Navigate to the license file you want to use, and click **Open**.
10. On the User Management screen, click **Finish**.
11. Close the Agfa Security Wizard.

Updating the secondary Application Server's hostname

(Topic number: 120308)

Use the Agfa Security Wizard to update the hostname on each server in a load-balance cluster.

To update the secondary Application Server's hostname

1. Log into secondary Application Server.
2. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Security Wizard**.
3. In the Security Wizard, select **Work with the Application Server default settings** and click **Next**.
4. On the Web Services Url Configuration screen, in the Hostname field, enter the enterprise URL and click **Update**. Click **Next**.
5. On the User Management screen, select **Do not add Administrator**. Click **Next**.
6. Select **No Administration License**.
7. Click **Finish**.
8. Close the Agfa Security Wizard.

Configuring the enterprise URL on the Application Server

(Topic number: 119487)

In a load-balanced environment, set the enterprise URL on the Application Server.

Note:

Do this task on both the primary and secondary Application Server in the cluster.

To configure the enterprise URL on the Application Server

1. Log into the primary or secondary Application Server.
2. Select **Start** > **All Programs** > **AgfaHealthcare** > **Business Services** > **Configuration Tool**.
3. Switch to the **Web Services** tab.
4. Under General Web Service Settings, in the Enterprise URL Hostname field, type the enterprise URL.

The enterprise URL is set.

Editing the login message in the primary Application Server's web.config file

(Topic number: 119492)

To allow a user to identify which Application Server is being accessed from the IMPAX Client, change the login message in the primary Application Server's web.config file to the name of the primary Application Server.

To edit the login message in the primary Application Server's web.config file

1. On the primary Application Server, navigate to:

   E:\wwwroot\AgfaHC.User.Security.Web.Services

2. Open the **web.config** file.
3. Search for the following text:

   ```
   <LoginMessage>
   ```

4. Edit the text within the <LoginMessage> element so that it contains the name of the primary Application Server server, as in the following example:

   ```
   <LoginMessage>Thank you for choosing Agfa. You are connected to
   PrimaryApplicationServerName</LoginMessage>
   ```

   where *PrimaryApplicationServerName* is the fully qualified domain name of the primary Application Server.

The login message includes the name of the primary Application Server.

Copying an SSL certificate to another Application Server

(Topic number: 11427)

Only SSL certificates that have been requested for a load-balanced environment can be copied to another Application Server. This task is applicable only to clusters with a load balancer.

To copy an SSL certificate to another Application Server

1. Add the SSL certificate on the primary Application Server (refer to page 163).
2. Add the certificates MMC snap-in tool (refer to page 164).
3. Export the SSL certificate from the primary Application Server (refer to page 164).
4. Import the SSL certificate (refer to page 165).

Adding the SSL certificate on the primary Application Server

(Topic number: 66943)

An SSL certificate uniquely identifies individuals and servers and is used for web server security.

To add the SSL certificate on the primary Application Server

1. Launch the Security Wizard.
2. Select **Work with SSL certificates**. Click **Next**.
3. Select **Import a certificate from a file**. Click **Next**.
4. To locate the certificate file, click **Browse** and navigate to the certificate file.

5. Click **Open**.
6. Click **Finish**.

The certificate is installed on the primary Application Server.

Adding the Certificates MMC snap-in tool

(Topic number: 50250)

The Certificates MMC snap-in tool provides a method of obtaining and managing certificates in Windows.

To add the Certificates MMC snap-in tool

1. On the primary Application Server, select **Start** > **Run**.
2. In the Run dialog, type

   mmc
3. In the Console1 dialog, select **File** > **Add/Remove Snap-in**.
4. In the Add/Remove Snap-in dialog, click **Add**.
5. From the list of snap-ins, select **Certificates** and click **Add**.
6. In the Certificates snap-in dialog, select **Computer account**. Click **Finish**.
7. In the Select Computer dialog, select **Local Computer** and click **Finish**.

Exporting an SSL certificate

(Topic number: 50253)

To copy an SSL certificate from the primary Application Server to the secondary Application Server, it must be exported.

To export an SSL certificate

1. Ensure that an exportable SSL certificate is installed on the primary Application Server.
2. On the primary Application Server, select **Start** > **Run**.
3. In the Run dialog, type

   mmc
4. In the Console dialog, double-click **Certificates** (**Local Computer**).
5. Navigate to **Personal** > **Certificates**.
6. From the list of certificates, select the certificate to be exported.
7. Right-click the certificate and select **All Tasks** > **Export**.
8. In the Welcome to the Certificate Export Wizard dialog, click **Next**.
9. In the Export Private Key screen, select **Yes, export the private key** and click **Next**.

10. In the Export File Format screen, select **Personal Information Exchange - PKCS #12 (.PFX)**.
11. Clear the **Delete the private key if the export is successful** checkbox.
12. Select the **Include all certificates in the certification path if possible** and **Enable strong protection (requires IE ...)** checkboxes.
13. Click **Next**.
14. In the Password dialog, enter a password to protect the certificate.
15. In the File to export dialog, enter a filename for the exported certificate, and save it to a location accessible by the secondary Application Servers. Click **Next**.
16. Click **Finish**.

Importing SSL certificates

(Topic number: 119719)

On the secondary Application Server, import the SSL certificate that was exported from the primary Application Server.

Importing an SSL certificate on Windows 2003

(Topic number: 66940)

Import the SSL certificate exported from the primary Application Server onto the secondary Application Server.

To import an SSL certificate on Windows 2003

1. On the secondary Application Server, select **Start** > **Run**.
2. In the Run dialog, type

   mmc
3. In the Console1 dialog, select **File** > **Add/Remove Snap-in**.
4. In the Add/Remove Snap-in dialog, click **Add**.
5. From the list of snap-ins, select **Certificates**. Click **Add**.
6. In the Certificates snap-in dialog, select **Computer account**. Click **Next**.
7. In the Select Computer dialog, select **Local Computer**. Click **Finish**.
8. In the Add Standalone Snap-in dialog, click **Close**.
9. In the Add/Remove Snap-in dialog, click **OK**.
10. In the Console Root window, expand **Certificates (Local Computer)**.
11. Expand **Personal (Console Root, Certificates, Personal)**.
12. Right-click **Certificates (Console Root, Certificates, Personal)** and select **All Tasks** > **Import**.
13. In the Certificate Import Wizard, click **Next**.
14. Click **Browse**.

15. Update the Files to Type box criteria to **All File**(***.***).
16. Navigate to and select the exported **.pfx** certificate from the primary Application Server. Click **Open**.
17. Click **Next**.
18. In the Password dialog, enter the password identified when exporting the certificate. Click **Next**.
19. In the Certificate Store dialog, click **Browse**.
20. In the Select Certificate Store dialog, select **Show physical stores**.
21. Expand **Personal** and select **Registry**. Click **Next**.
22. Click **Finish**.

    The certificate is imported onto the additional Application Server.
23. Assign the certificate to the IIS service.

Importing an SSL certificate on Windows 2008

(Topic number: 119721)

Import the SSL certificate exported from the primary Application Server onto the secondary Application Server.

To import an SSL certificate on Windows 2008

1. On the secondary Application Server, select **Start** > **Run**.
2. In the Run dialog, type

   mmc
3. In the Console1 dialog, select **File** > **Add/Remove Snap-in**.
4. In the Add or Remove Snap-ins dialog, under Available Snap-ins, select **Certificates** and click **Add**.
5. In the Certificates snap-in dialog, select **Computer account**. Click **Next**.
6. In the Select Computer dialog, select **Local Computer**. Click **Finish**.
7. In the Add or Remove Snap-ins dialog, click **OK**.
8. In the Console Root window, expand Certificates (Local Computer).
9. Right-click **Personal** (**Console Root, Certificates, Personal**) and select **All Tasks** > **Import**.
10. In the Certificate Import Wizard, click **Next**.
11. Click **Browse**.
12. Update the Files to Type criteria to **Personal Information Exchange** (***.pfx;*.p12**).
13. Navigate to and select the exported **.pfx** certificate from the primary Application Server. Click **Open**.
14. Click **Next**.

15. In the Password dialog, enter the password identified when exporting the certificate. Click **Next**.
16. In the Select Certificate Store dialog, select **Place all certificates in the following store**. Click **Next**.
17. Click **Finish**.
18. In the dialog displaying the message `The import was successful`, click **OK**.
19. Assign the certificate to the IIS service.

Replicating the AD LDS database between two Windows 2008 servers in a workgroup

(Topic number: 120314)

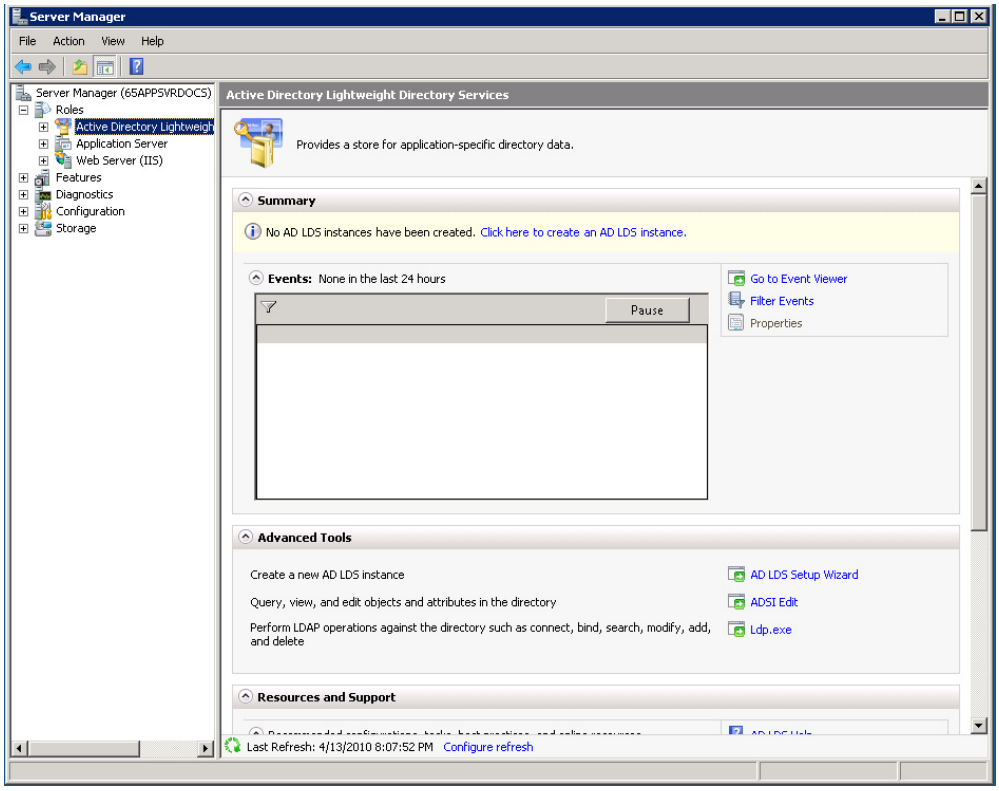
When setting up Application Servers in a load-balanced environment, you can set up AD LDS replication when each Application Server in the cluster is part of a workgroup.

Note:

The user account you use to set up the replication must exist on both Windows 2008 servers and must have the same password.

To replicate the AD LDS database between two Windows 2008 servers in a workgroup

1. Log into the Windows 2008 Application Server as an administrator.
2. Select **Start** > **Server Manager**.
3. Expand **Roles** and select **Active Directory Lightweight Services**.



4. Under Advanced Tools, click **AD LDS Setup Wizard**.
5. In the Active Directory Lightweight Directory Services screen, click **Next**.
6. In the Setup Options dialog, select **A replica of an existing instance**. Click **Next**.
7. In the Instance Name dialog, type **AgfaHealthcare**.

Important!

The name of the replicated instance must be identical to the original instance on the other Windows 2008 server you are using for replication.

8. Click **Next**.
9. In the Ports screen, accept the default LDAP port number (389) and SSL port number (636). Click **Next**.
10. In the Joining a Configuration Set screen, type the fully qualified domain name and LDAP port number of the AD LDS LDAP instance that you are using for the replication.
11. In the Administrative Credentials for the Configuration Set screen, accept the default value **Currently logged on user**. Click **Next.**
12. Click **Next**.
13. In the Copying Application Directory Partitions screen, select the **CN=healthcare,DC=agfa,DC=com** partition. Click **Next**.

14. In the File Locations screen, in the Data Files and Data Recovery files fields, accept the default settings and click **Next**.
15. On the Service Account Selection screen, select **This account** and click **Browse**.
16. In the Select User screen, under Enter the object name to select, type **AgfaService**. Click **Check Names** and then click **OK**.
17. In the Service Account Selection screen, type the password for the AgfaService account. Click **Next**.

    If a confirmation message is displayed, click **Yes**.
18. On the AD LDS Administrators screen, accept the default values. Click **Next**
19. On the Ready to Install screen, click **Next**.

    The installation process takes a few minutes to complete.
20. When the installation is complete, click **Finish**.
21. Restart the server.

Configuring the load balancer for the Instant Messaging feature

(Topic number: 125768)

The Instant Messaging feature allows users to connect easily with other users in the IMPAX Client.

The Instant Messaging feature uses https (port 443) to ensure that communication is encrypted. To use this feature in a load-balanced environment, you need to make the following changes.

Note:

We assume a basic load balancer setup was done prior to performing these steps.

To configure the load balancer for the Instant Messaging feature

1. For port 443/tcp (https), on the load balancer increase the session lifetime from 160 seconds to 900 seconds.
2. Messaging over http (port 80) has been deprecated (formerly it was set to 60 minutes) on the load balancer. Disable load balancing for this port.

Troubleshooting IMPAX Application Server

D

As you install the Application Server, you may encounter various installation problems.

Troubleshooting: The Application Server software upgrade fails when using a different administrator user account

(Topic number: 131733)

Issue

The Application Server upgrade fails if the same administrator user account is not used when performing an upgrade.

Details

The Application Server upgrade fails when an administrator user account, different from the one used during installation, is used to upgrade the software. The installer package starts running and displays the following error: Error 1721. There is a problem with this Windows Installer package. A program required for this install to complete could not be run. Contact your support personnel or package vendor.

Solution

Use the same administrator user account applied during the installation when performing a software upgrade of the Application Server.

Troubleshooting: The Application Server installation or upgrade fails to register ODP .NET

(Topic number: 118893)

Issue

The Application Server installation or upgrade fails to register ODP .NET with the warning `Expected ODP.NET 2.102 was not found` and the Application Server installation/upgrade eventually fails.

Details

ODP .NET cannot be registered if an unsupported version of Oracle is installed on the Application Server, causing the installation/upgrade of the Application Server to fail.

Solution

1. Uninstall the version of Oracle (refer to page 131).
2. Install the supported version of Oracle (refer to page 132).

   Note:

   If installing the Application Server at a SQL site and connecting to the IMPAX RIS, you must install the supported version of Oracle.

3. Install (refer to page 49) or upgrade (refer to page 135) the Business Services.

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 150) 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: Poor performance on the Application Server

(Topic number: 11205)

In this situation, Clients experienced longer-than-normal wait times for responses to web requests.

Issue

The Application Server is performing slowly.

Details

The Buffer Overflow Protection in McAfee antivirus software causes significant performance problems on the Application Server and all Clients attached to it. Other antivirus software may cause similar problems if it contains similar buffer overflow protection.

Solution

Microsoft and McAfee recommend disabling the **Buffer Overflow Protection** option.

To disable the Buffer Overflow Protection option

1. Open the McAfee VirusScan Console.
2. Select the **Buffer Overflow Protection** entry and disable it.
3. If the enterprise has ePO or Protection Pilot enabled (also McAfee products) then make the change on those systems too; otherwise, the setting may revert after a few minutes.

Troubleshooting: Login problems

(Topic number: 11261)

Issue

Cannot log into the Application Server.

Details

When troubleshooting login problems, to attempt to determine where the problem is, perform the following tasks:

1. Review the Server log files.
2. Check the status when logging in.
    a. On the Application Server, in a browser, navigate to this location:

    https://localhost/AgfaHC.User.Security.Web.Services/login.asmx

    b. Enter the username and password for the administrator.
    c. Select **Login**.
    d. Under Test, click **Invoke**.
    e. In the results, if Status="failure", an authentication problem exists.

Solution

To attempt resolve the problem, configure the following settings:

1. In IIS, disable the Windows Authentication for Default Web Site and AgfaHC.User.Security.Web.Services.
2. Enable non-https login access in E:\AgfaHC.User.Security.Web.Services\web.config by modifying the SecureLoginRequired setting to **false**.
3. If when using ADSI Edit to change the password an error indicating that this could not be done is displayed, non-SSL ADSI access may need to be enabled. Refer to the ADAM SDK kit in the file start_here.htm for details.

Troubleshooting: A certificate is already installed error displayed on the Application Server

(Topic number: 55034)

Issue

When configuring a new application server and the user is installing a new SSL certificate, the message `A certificate is already installed` is displayed.

Details

When Application Servers are staged, an SSL certificate is installed onto the computer to complete the initial staging. Usually this SSL certificate has an expiry date, but if the SSL certificate has not expired when the new SSL certificate is installed, the message `A certificate is already installed` is displayed.

Solution

Remove the existing SSL certificate from the Application Server, and then install the new SSL certificate.

To remove the existing SSL certificate

1. On the Application Server, open Internet Explorer.
2. Select **Tools** > **Options**.
3. Switch to the **Contents** tab.
4. In the Certificates area, click **Certificates**.
5. In the Certificates dialog, switch to the **Trusted Root Certification Authorities**.
6. Select the SSL certificate to be removed from the list. Click **Remove**.
7. In the warning dialog, click **Yes**.

   The old SSL certificate is removed from the Application Server.

Troubleshooting: No license available

(Topic number: 11276)

Issue

When I try to log into the IMPAX Client, I get the message `No license available`.

Details

This error message may have two possible causes:

- The role of the user attempting to log in has been assigned a demo license, and that license has expired.
- No licenses are available to allocate to the role. All the licenses are in use, and have not been released when users log out of IMPAX.

Solution

Solution #1: Demo license has been assigned to a role

1. Request a new license for the role, using the correct MAC address, through licensekey@agfa.com.

Solution #2: All licenses currently being used

1. Release all the licenses from user roles.

Troubleshooting: Cannot install administrator license

(Topic number: 11359)

Issue

When I am installing the administrator license through the Security Wizard, I get the error message `Unable to install administrator license`.

Details

This error message occurs when the license failed the integrity check or the license is already installed.

A license fails the integrity check when the contents of the license file are modified, the expiry date is changed, or the formatting of the license is broken. When this is the problem the error `License key did not pass integrity check` is present in the Security Wizard log file.

If the license is already installed, you must uninstall the license before installing it a second time. When this is the problem with the license, in the Security Wizard log file, the error `License is already installed` is present.

Solution

Solution #1: License fails the integrity check

1. Request a new Administrator license for the Application Server, using the correct MAC address, through licensekey@agfa.com.
2. Uninstall the license (refer to page 85) causing the errors.
3. Install and activate the new administrator license (refer to page 84).

Solution #2: License is already installed

Install the license using the Service Portal.

1. Uninstall the administrator license (refer to page 83).
2. Install and activate the administrator license (refer to page 80).

Solution #3: License is already installed

Install the license using the License Manager.

1. Uninstall the administrator license (refer to page 85).
2. Install and activate the administrator license (refer to page 84).

Troubleshooting: Cannot assign license to Administrator role

(Topic number: 11358)

Issue

When I try to activate the Administrator license using the Security Wizard, I get the message `Unable to assign license to Administrator role`.

Details

The Administrator license installs correctly, but when you try to activate the license, the error message is displayed. In the Security Wizard log file, the error `Hardware key not present` is present. IMPAX generates this error when the MAC address in the license does not match the MAC address of the computer the license is being activated on.

Solution

1. Request a new Administrator license for the Application Server, using the correct MAC address, through licensekey@agfa.com.

Troubleshooting: Could not establish trust relationship with remote server

(Topic number: 11361)

Issue

I try to launch the IMPAX Client, nothing happens and the login never appears. The log file contains a `Could not establish trust relationship with remote server` error.

Details

When you have problems with the SSL certificate, or the certificate has expired, the following error message appears in the log file:

```
ERROR 2010-08-23 11:09:21,281 [MainThread] AgfaHC.Pacs.Application.ImpaxClient
[] - HandleUnhandledException(): Unhandled exception:
AgfaHC.Web.Services.Proxy.SoapProxyBaseException: The underlying connection was
closed: Could not establish trust relationship with remote server.
```

Solution

1. Request a new certificate.
2. Import and assign the SSL certificate (refer to page 64) on the Application Server.

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 (refer to page 29).

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: 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: Dell 2950 with Windows 2003 server restarting instead of shutting down

(Topic number: 66126)

Issue

When shutting down a Dell 2950 with Windows 2003 server installed, the system restarts instead of shutting down.

Details

Two possible causes of this problem are:

1. The computer may be set to restart automatically.
2. The NIC driver may need to be updated.

Solution

If the computer is set to restart automatically, change the setting.

To change the restart settings

1. Open the Windows System properties.

2. Switch to the **Advanced** tab.
3. Under Startup and Recovery, click **Settings**.
4. Under System failure, clear the **Automatically restart** checkbox.
5. Click **OK** twice.

This may solve the problem. If not, you may need to update the NIC drivers.

To update the NIC drivers

1. Download the executable NIC_DRVR_WIN_R196231.EXE from the Dell website at:

   http://support.us.dell.com/support/downloads/download.aspx?c=ca&l=en&s=gen&releaseid=R196231&formatcnt=1&libid=0&fileid=271118
2. Run the install executable, according to Dell's instructions.

Troubleshooting: Not all printer log entries are listed in the Application Server log file

(Topic number: 128552)

Issue

Not all of the printer log entries are listed in the Application Server log file.

Details

The following entries should be listed in the AgfaHC.Pacs.Web.Services.log file:

- PrinterService.GetAllTemplates
- PrinterConfigInstalledDac.Fill
- Printer.GetListOfInstalledPrinters
- PrinterService.GetListOfInstalledPrinters

After an upgrade, calls to the Application Server are not made due to Client caching. This causes entries in the Application Server log to be dropped.

Solution

To ensure all calls are being made to the Application Server after an upgrade, clear the Client cache.

To clear the Client cache

1. Log out of the IMPAX Client.
2. Close the Login dialog.
3. To launch the IMPAX Client, select **Start** > **All Programs** > **Agfa IMPAX** > **IMPAX Client**.
4. Log into the Client.

External software licenses

E

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)

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

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.]

*/

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

ADAM

Active Directory Application Mode. Directory services for an individual application that controls user login and privilege information.

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.

ADT

Admission, Discharge, Transfer. An ADT message contains patient demographic and visit information that is stored by a HIS or RIS.

Application Server

Intermediary server between IMPAX Client and IMPAX Server machines. LDAP, Documentation, and other Business Services reside on the Application Server.

Archive Server

The IMPAX server that manages the archive. The Archive Server handles requests to store studies to the archive and to retrieve studies from the archive. The Archive Server stores studies in its cache before archiving them to long-term storage.

B

Business Services

The data pipelines that IMPAX Clients use to get PACS information. The Business Services reside on the IMPAX Application Server or Servers.

C

cluster

A networking solution combining two or more otherwise independent computers, enabling them to work together in managing hospital data.

Connectivity Manager

A middleware component in the integration between hospital information systems and other hospital imaging departments. Connectivity Manager also provides connectivity to each modality and the PACS.

D

database

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

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.

H

HIS

Hospital Information System. The database used by a hospital to manage patient information and scheduling.

HIS verification

An option that forces the PACS to verify all incoming images from an acquisition station or modality against specific criteria, such as the patient ID and accession number. The PACS sends a message through the RIS Gateway to verify the criteria against what is contained in the HIS. If the criteria match, then the images can be stored permanently.

HL7

Stands for Health Level 7, a standard communication protocol used for the transmission of medical information. HL7 is used primarily by HIS systems and does not support transmission of images.

host name

The host name is a common alphanumeric alias for the IP address of a server.

HTTP

Hypertext transfer protocol, a TCP-based protocol for transferring hypertext requests and information between servers and browsers.

I

IHE

Stands for Integrating the Healthcare Enterprise. IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care.

IP address

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

L

LDAP

Lightweight Directory Access Protocol, the technology for storing user names and IDs, passwords, and user-related preferences. This information is stored in an LDAP depository.

load balancing

Distributing processing and communications activity evenly across a computer network so that no single device is overwhelmed.

M

MAC address

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

master Curator

When using multiple Curators, the first Curator that runs, which owns the job queue.

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.

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.

P

PACS

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

R

RIS

Radiology Information System. Responsible for scheduling exams and for report management in the Radiology department.

role

A collection of users or other roles that holds IMPAX Client permissions and preferences as well as licensing options. For example, a role can represent the enterprise, the institution, a department, or a team.

S

single-host configuration

A configuration in which the Database, Archive Server, and Network Gateway server components are all installed on a single server.

single-server configuration

An IMPAX single server is a Windows server that runs the AS300 Server software in a single-host configuration along with the Application Server and Connectivity Manager software.

slave Curator

When using multiple Curators, the secondary Curators. Though the master Curator owns the job queue, PREPARE jobs are associated with the Curator that started the job.

SSL

Secure Sockets Layer. A protocol from Netscape Communications Corporation, which is designed to provide secure communications on the Internet.

SSL certificate

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

standalone station

Windows server on which the IMPAX Client, AS300, and Application Server software are installed. Runs under Windows XP SP3. The standalone does not have its own installation program. To create a standalone , the AS300, Application Server, and Client installation programs are each run separately.

U

user

Users represent individuals, such as a radiologist or a clinician. Each user must

belong to at least one primary role. A user can also belong to other secondary roles. Users inherit permissions, licenses, and preferences from their role.

W

web cache

Images that have been compressed by Curator are stored in the web cache. These images are compressed using Mitra Wavelet compression to reduce their size for access over low bandwidth.

Web Service

A component that runs on a web server and allows programs to request and receive data over HTTP or HTTPS.

wizard

Wizards are used to automate processes. Wizards perform a predetermined sequence of actions after they are selected and applied.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z