AS300 Installation and Configuration Guide

IMPAX 6.5.1

Installing and Configuring the AS300 Components or Upgrading IMPAX from a Single-Host to Multi-Host Configuration

AGFA

see more | do more

Copyright information

Trademark credits

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

Additional trademark credits

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

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 - 14

Manufacturer's responsibility

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

- Installation, modifications, adjustments, changes, or repairs are performed by suitably qualified service personnel.

- The electrical installation of the site in which the equipment is used is according to an applicable safety standard (UL, CSA, or IEC/CDE).
- The equipment is used according to the instructions provided in the operation manuals.
- 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.

External software licenses

(Topic number: 7696)

Information about third-party software licenses and copyrights can be found in *External software licenses* (refer to page 144).

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

To successfully install IMPAX, servers must meet certain hardware and software requirements.

The IMPAX server configuration to use must also be determined.

Attention: An archive is necessary to prevent permanent data loss

(Topic number: 98632)

Data archiving is an essential component of a PACS system. IMPAX Autopilot manages data in the cache and ensures that it does not run out of disk space. As the cache nears capacity, Autopilot deletes images to make space available for incoming images, usually on a first in, first out basis but ultimately governed by user-defined criteria. In addition to the automated cache management, users with the necessary permission can delete images from the cache.

For details about Autopilot configuration, refer to "Autopilot Management" (topic number 9129) in the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*. For details about permissions, refer to "Defining permissions" (topic number 9451) in the Administering IMPAX component of the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Under normal circumstances in which an archive is employed, any data that is deleted from the cache is stored on the archive and no permanent data loss occurs. If, however, an archive is not employed, data deletion results in a permanent loss of the record unless that data has been exported and/or stored elsewhere.

CAUTION!

Although IMPAX can be used without an archive, we highly recommend an archive be used to prevent data loss. It is the responsibility of any IMPAX customer to recognize and accept these conditions. In addition, granting the permission to delete an image or study from the

cache must be carried out with the understanding of the risk it can pose with regard to the permanent loss of patient data.

Prerequisite knowledge: IMPAX installations

(Topic number: 7633)

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

What is IMPAX?

(Topic number: 6910)

IMPAX is an image archiving and communications system that eliminates the need for film because it receives, distributes, archives, and displays images. IMPAX automates the flow of information to integrate the Radiology department with the rest of the hospital. IMPAX can also integrate remote locations such as clinics or home offices to the system for offsite viewing of images.

Additional IMPAX documentation

(Topic number: 6911)

This guide is intended for service and administrative personnel who are installing or upgrading, configuring, and maintaining the Server components of the IMPAX 6.5.1 system.

For information about using the IMPAX software once it is installed, refer to the *IMPAX 6.5.1 Server Knowledge Base*, *IMPAX 6.5.1 Application Server Knowledge Base*, and *IMPAX 6.5.1 Client Knowledge Base: Extended*. These Knowledge Bases are installed on the Application Server. Refer to "Installing the IMPAX documentation" (topic number 15523) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Opening the IMPAX 6.5.1 Server Knowledge Base

(Topic number: 58560)

Follow this procedure to open the IMPAX 6.5.1 Server Knowledge Base.

To open the IMPAX 6.5.1 Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed.
2. Launch the IMPAX Administration Tools and log in. Select **Help** > **Help URL**. On the IMPAX Documentation page, click the **IMPAX Server Knowledge Base** link.

or

From a browser on a connected computer, navigate to https://*app_server_name*/impax/documents/server/default.htm

Opening the IMPAX 6.5.1 Application Server Knowledge Base

(Topic number: 58563)

Follow this procedure to open the IMPAX 6.5.1 Application Server Knowledge Base.

To open the IMPAX 6.5.1 Application Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed.
2. On the Application Server, double-click the **AGFA IMPAX Knowledge Base** desktop shortcut. Select the **IMPAX Application Server Knowledge Base** link.

   or

   From a browser on a connected computer, navigate to https://*app_server_name*/impax/documents/appserver/default.htm

Opening the IMPAX 6.5.1 Client Knowledge Base: Extended

(Topic number: 58566)

Follow this procedure to open the IMPAX 6.5.1 Client Knowledge Base: Extended.

To open the IMPAX 6.5.1 Client Knowledge Base: Extended

1. Ensure that the IMPAX documentation has been installed.
2. Launch the IMPAX Client application and log in.
3. Press **F1**.

Components of the IMPAX cluster

(Topic number: 7091)

Every IMPAX 6.5.1 installation comprises the following main components:

- Database Server hosting the Oracle or SQL database

  The database used by the IMPAX 6.5.1 cluster. It collects, organizes, and manages all patient and study demographic data that is contained in DICOM header files. Installation of a Database Server is covered in this guide.

- Network Gateway

Workflow manager of the IMPAX 6.5.1 cluster. It receives studies from modalities and provides DICOM security and validation. Installation and configuration of a Network Gateway is covered in this guide.

- Archive Server

  DICOM archive used for permanent storage and retrieval of studies. Installation and configuration of an Archive Server is covered in this guide.

  Although IMPAX can be used without an archive, we highly recommend an archive be used to prevent data loss. For further information, see *Attention: An archive is necessary to prevent permanent data loss* (refer to page 9).

- Application Server

  Clients connect to one or more Application Server machines, which act much like a proxy machine to handle security, authentication, and communication with the IMPAX 6.5.1 Server components. Installation and configuration details are covered in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

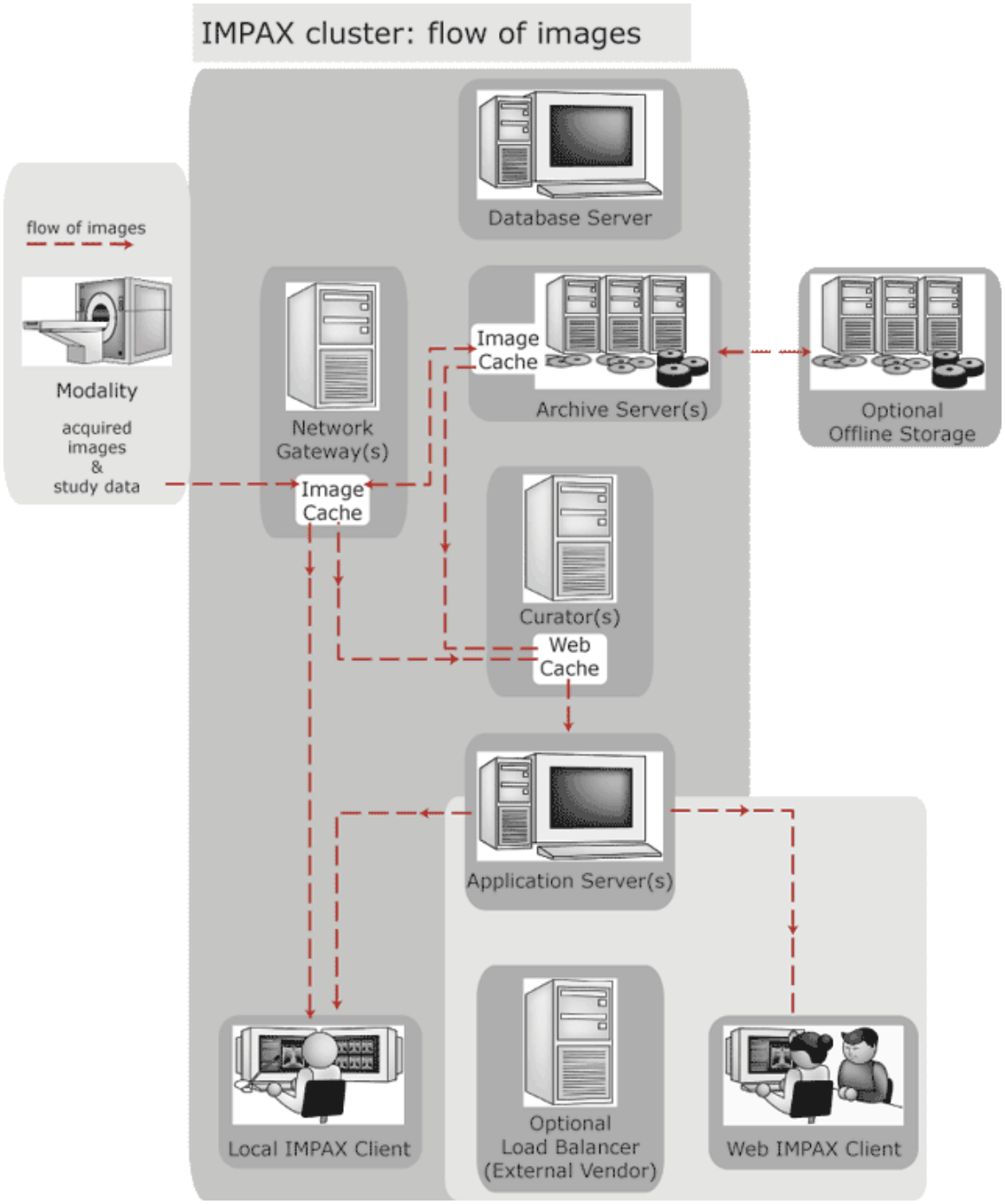
- Curator

  Clients can view JPEG compressed or wavelet compressed DICOM images generated by the Curator. Installation and configuration details are covered in the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*.

- Clients—Local and remote

  Multi-modality diagnostic or clinical display station for viewing images and diagnosing studies. Installation and configuration details are covered in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

The sum of these components is called the *cluster*. The IMPAX 6.5.1 cluster is the set of components that are controlled by one Oracle or SQL database. The Database Server must be installed first because the other stations must connect to the Oracle or SQL database.



IMPAX clusters also include a Connectivity Manager component. 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 IMPAX. These systems often speak different languages, or protocols. PACS and modalities typically speak DICOM, while hospital information systems generally speak HL7.

Single-cluster configurations

(Topic number: 6916)

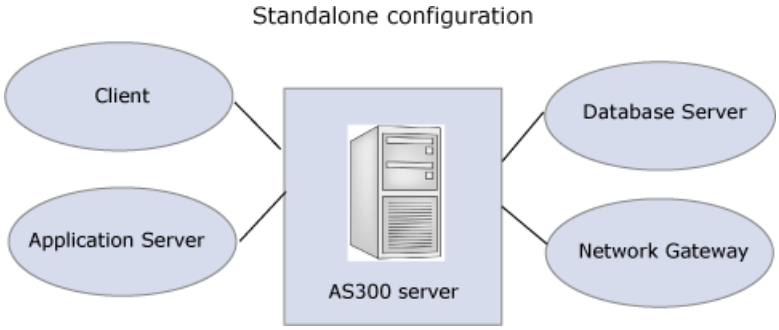
The components of a cluster can be distributed in various ways. A typical institution has a Database Server, one or more Archive Servers, one or more Network Gateways, one or more Curators, and one or more Application Servers. Clients are spread throughout the entire enterprise and through remote connection. A single IMPAX cluster can service one or more healthcare facilities and, in such an environment, IMPAX can HIS verify against and access reports from multiple Connectivity Managers for multiple RIS domains.

Note:

The Archive and Archive Server are the same thing. The archive station is the archive on its own machine. Both are part of the IMPAX cluster.

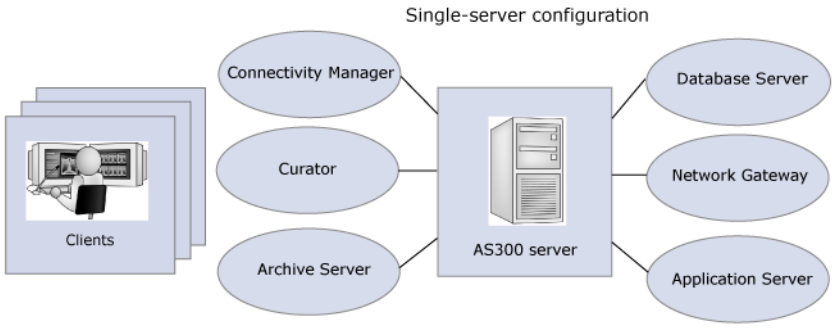
Standalone

In a standalone configuration, AS300 Server, Application Server, and Client components are installed on the same computer. The standalone station can be used for diagnostic or non-diagnostic purposes. New installations run under Windows 7 with an Oracle for Windows database. Using VMware Player, the AS300 Server and Application Server components run on Windows 2008 Server. Existing configurations can continue to run under Windows XP and with a SQL Server 2005 or 2008 database. Refer to the *IMPAX 6.5.1 Standalone Installation and Configuration Guide* or to the *IMPAX 6.5.1 Standalone Upgrade Guide*.



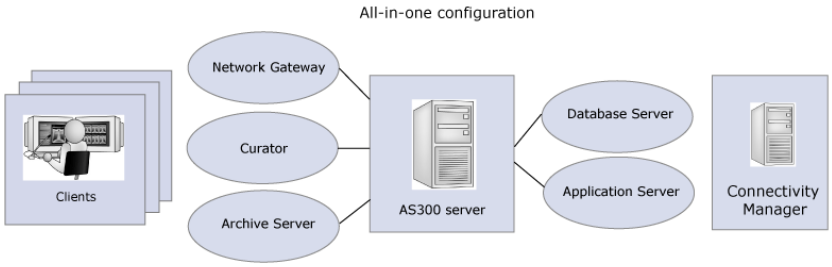
Single-server

In a single-server configuration (refer to page 120), all AS300 Server, Application Server, and Connectivity Manager components are installed on the same Windows computer with an Oracle for Windows database using VMware; Clients are installed on other computers.



All-in-one

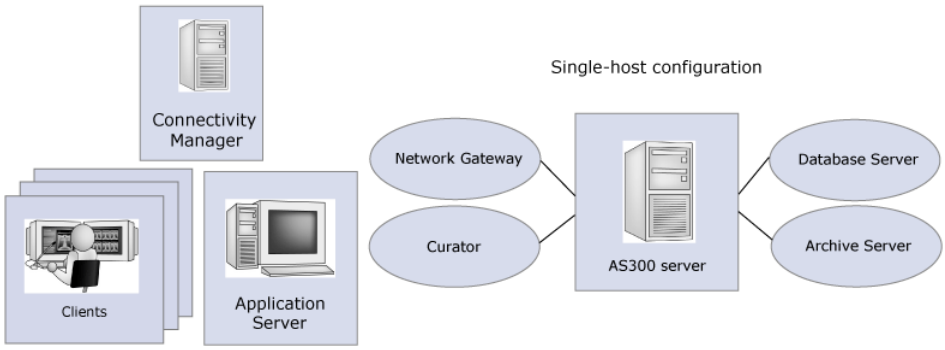
In an all-in-one server configuration, all AS300 Server and Application Server components are installed on the same Windows computer with an Oracle for Windows database.



Single-host

In a single-host configuration, the AS300 or AS3000 Server Database, Archive Server, and Network Gateway components are all installed on one "box" or station, with the Application Servers, Clients, and Connectivity Manager each installed on separate stations.

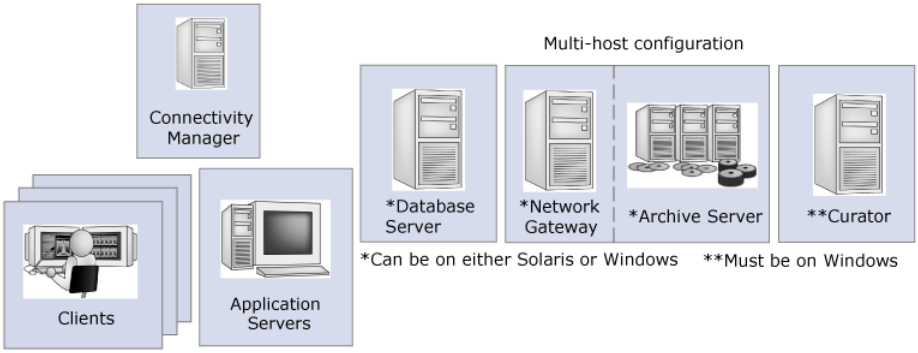
In an AS300 single-host configuration, Curator can also be installed on the same station as the Server components; however, in an AS3000 single-host configuration, Curator must be separately installed. The Curator component runs only on the Windows operating system.



Multi-host

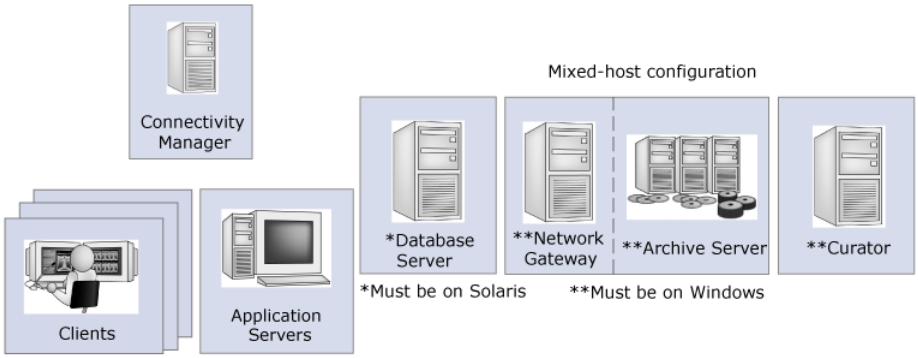
In a multi-host configuration, each Server component is installed on its own station: the Database Server is installed on a separate computer from the Archive Server. The Network Gateway component may either be installed on yet another server, or installed along with the Database Server or Archive Server.

By installing the Server components onto separate stations, workflow volume is better managed and system performance enhanced.



Mixed-host

In a mixed-host configuration, an AS3000 Database Server is combined with an AS300 (Windows-based) Archive Server, Network Gateway, and Curator server.



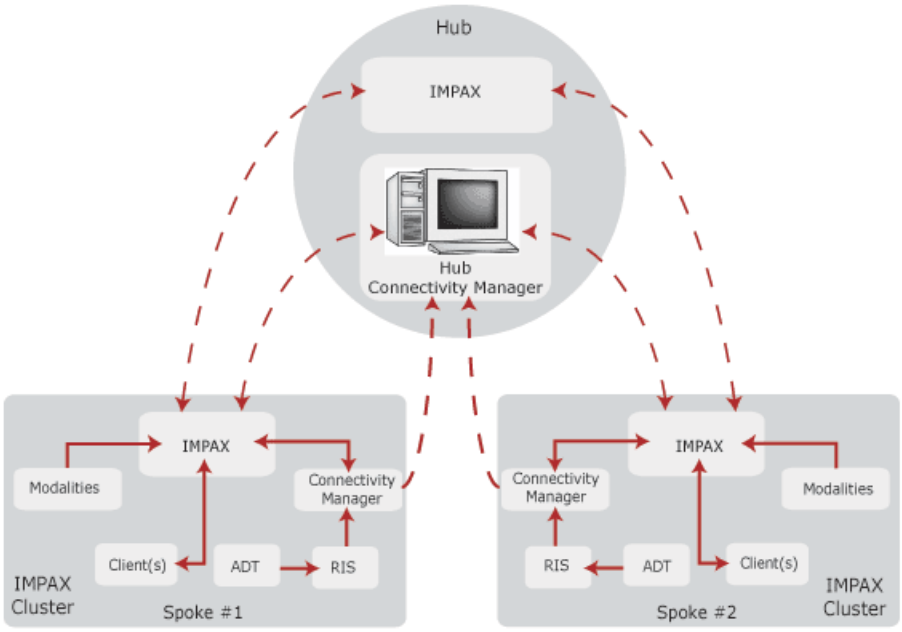
Multiple IMPAX cluster configurations

(Topic number: 10378)

IMPAX can optionally be run in a multiple IMPAX cluster configuration. This configuration provides a patient-centric view across hospitals within several sites. This view is delivered by extending the scope of study query, study retrieval, and data synchronization from a single hospital site to several hospital sites that have multiple patient domains (multiple RISs) in one or more IMPAX clusters.

Central to the multiple IMPAX cluster configuration is the MVF-based data center component. The data center provides storage for studies through the Archive Server, as well as retrieval of the study data. Connected to the data center are a collection of hospital groups known as *entities*, each with a local PACS infrastructure. Most entities use IMPAX as their PACS system.

The relationship between the data center and the various clusters is characterized as a *hub and spoke*. The data center (*hub*) serves or archives data from the entities, known as *spokes*.



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 120) in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

All documentation is available on the IMPAX Documentation DVD.

IMPAX AS300 Server hardware and software requirements

(Topic number: 6674)

The following lists the hardware and software requirements for an IMPAX AS300 Server (including single-server configurations). Where a specific manufacturer is identified, only that manufacturer's device is supported.

IMPAX Server: Hardware requirements

(Topic number: 6690)

The following hardware configuration is recommended for IMPAX AS300 servers (including single-server configurations).

Important!

When installing or upgrading to IMPAX 6.5.1 on Windows machines, all Servers and Application Servers must have Pentium 4 or later CPUs. CPUs previous to 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
Example systems	**Preferred:** HP ML370, DL380 (may be deployed with VMware ESX 3.5) **Supported:** Dell 1900, 2900, 2950, 6900*, 6950* Stratus® ftServer® 4300, 4410, or 5700 (dual CPU)
Hard drive	Minimum three drives Minimum drive size 40 GB Minimum drive size 73 GB NAS/SAN connections also supported
RAM	4 GB minimum
Number of CPUs	Two or four* CPUs, 2 GHz minimum each
RAID	Embedded RAID (for onboard storage)
Tape backup	DAT 72 tape drive, if required for database backup
Video	Integrated video
DVD	Yes
Network interfaces	100/1000 Mbps
Modem	N/A
Power supplies	Redundant (additional)
Peripherals	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.

Additional AS300 hardware requirements: Storage requirements

(Topic number: 6733)

Additional hardware can be used to meet archive requirements.

IMPAX AS300 Server: HSM storage requirements

(Topic number: 6686)

Note:

Direct attached libraries are not supported in IMPAX 6.5.1.

The following HSM storage devices are supported:

- EMC
- HP
- QStar

Note:

To use QStar HSM with IMPAX, open port 160 for UDP messages.

IMPAX AS300 Server: PACS Store and Remember archive requirements

(Topic number: 7123)

For PACS Store and Remember archiving, no additional hardware is required.

IMPAX AS300 Server: Storage requirements

(Topic number: 6616)

Manufacturer	Model	Manufacturer	Model
IBM	Shark ESS Series FastT Series	HP	MSA1000 series EVA series
NetApp	R series F series FAS series	Hitachi	9000 series
EMC	CX-3 series	StorageTek (STK)	D series

Manufacturer	Model	Manufacturer	Model
	Symmetrix DMX series		B series
	Centera		
	Centera Universal Access		

IMPAX AS300 Server: Non-SCSI CD/DVD burner and controller cards

(Topic number: 58044)

OEM-supplied CD/DVD writer

IMPAX Server: External software requirements

(Topic number: 6695)

The following software is required for most IMPAX AS300 servers. Unless otherwise indicated, Agfa does not provide the software as part of the IMPAX AS300 Server installation package.

Component	Requirements
Operating system	**For upgrades:** Windows Server 2003 R2 SP2, Standard or Enterprise Editions, 32-bit or 64-bit (only a dedicated Database Server can be run on Windows 64-bit) or **For new installs:** Windows Server 2008 SP2, Standard or Enterprise Editions, 32-bit or 64-bit (only a dedicated Database Server can be run on Windows 64-bit)
Database software	One of the following: • Oracle 10g 32-bit Server and Client (provided on Oracle for Windows 32-bit DVD) or • Oracle 10g 64-bit Server (provided on Oracle for Windows 64-bit DVD) or • Microsoft SQL Server 2005, Standard or Enterprise Edition, with Service Pack 3 (upgrades only) or Microsoft SQL Server 2008, with Service Pack 1 (upgrades only)
Browser	Internet Explorer 8.0
Java	

Component	Requirements
Documentation	Latest version of Adobe® Reader®
Remote access (optional)	Symantec pcAnywhere version 12.5
Antivirus	McAfee Antivirus 4.5 or higher

IMPAX AS300 installation programs

(Topic number: 7684)

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

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

Note:

SQL Server 2008 is not distributed with IMPAX but is available from the Agfa Parts Center.

32-bit AS300 installer packages reference

(Topic number: 7682)

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

Default

Default packages	Purpose
MVFCore	Installs the DICOM services for IMPAX and contains several core Windows services and database tables used by IMPAX.
MVFCache	Installs the DICOM SCU and autopilot services used by IMPAX and spftp services. MVFCache includes mvf_compressor, used for lossy compression, and cache_migration, used to migrate cache volumes from a flat to a hierarchical structure.
MVFNetworkGateway	Installs the SCP and APIP-SCP services used by IMPAX. Install this package only on stations that require Network Gateway functionality. Servers that support only internal transfers, not incoming DICOM communications, do not require it.
AdministrationTools	Installs the Java Administration Tools application for configuring and managing IMPAX. It also copies the Java Runtime Environment (JRE) self-extracting executable onto the system. This package is not available in the 64-bit installer, but must be installed as part of the IMPAX cluster. Therefore, if installing a 64-bit dedicated Database Server under Oracle, be sure to install this package on another AS300 server in the cluster. The package can be installed on more than one server, but run only one instance at a time (by disabling the other Administration Tools services).
MVFocr	Installs the files necessary to enable Optical Character Recognition. This is an optional installation that works in conjunction with the MVFNetworkGateway package. Install it only if your system requires OCR. The OCR package installs default OCR templates to handle many different modality vendors. OCR training tools are not included with IMPAX.
VaultAgfa	Includes specific requirements and database extensions. Not required on 64-bit systems.

Database

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

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

Archive

Archive packages	Purpose
MVFhsm	Installs the HSM package.

Archiving considerations:

- If the server is used for viewing only (no archiving), do not install any archive package.
- PACS Store and Remember archiving is available but does not require an installation package. It does require an archive license. For details on setting up PACS Store and Remember archiving, refer to the *IMPAX 6.5.1 Server Knowledge Base*.

Optional

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

Optional packages	Purpose
MVFCompressor	Installs the MVF Compressor package, which includes mvf_compressor_scheduler. The mvf_compressor_scheduler process is responsible for scheduling the lossy compression of images.
MVFCurator	Installs the Curator package. The Curator process compresses incoming images into Mitra wavelet format and stores them in the web cache. Studies compressed by the Curator process are served locally or over a network to display clients.
MVFcdexport	Installs the CD Export server, used with the CD Export feature in the IMPAX Client. The CD Export server processes local burn jobs created by the IMPAX Client and prepares the zip files containing the data for the burn job. For instructions on using CD Export, refer to "Exporting and viewing images from CD or DVD" (topic number 8209) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.
MVFchangeaccepter	Installs a package related to the processing of change context (cc) objects. This feature is not required and we recommend that this package not be installed.
MVFpap	Installs the PAP package. A PACS Archive Provider (PAP) acts like a Service Class Provider (SCP) by receiving studies and allows sites to have their studies mirrored at another site through PACS Store and Remember archiving. This mirroring protects against data loss and enables studies at one PACS to be viewed at another. For instructions on configuring a PAP, refer to "Configuring a PACS Archive Provider (PAP)" (topic number 11586) in the *IMPAX 6.5.1 Server Knowledge Base*.

Optional packages	Purpose
MVForadg	Installs a set of scripts and tools for configuring and monitoring Oracle Data Guard. Data Guard is Oracle's high-availability solution. **Important!** Data Guard works **only** on servers running Oracle Enterprise Edition. Do not install it on a database server using SQL Server or Oracle Standard Edition, and do not include it on other types of servers (Archive Server, Network Gateway, Curator, standalone).

64-bit AS300 installer packages reference

(Topic number: 65290)

The 64-bit IMPAX AS300 installer includes only the packages that can take advantage of the 64-bit processor. 64-bit IMPAX is for new installs only. Only dedicated Database Servers running Oracle can be installed using the 64-bit AS300 installer.

Default packages	Purpose
MVFCore	Installs the DICOM Services for IMPAX and contains several core Windows services and database tables used by IMPAX.

Optional packages	Purpose
MVForadg	Installs a set of scripts and tools for configuring and monitoring Oracle Data Guard. Data Guard is Oracle's high-availability solution. **Important!** Data Guard works **only** on servers running Oracle Enterprise Edition. Do not install it on a database server using SQL Server or Oracle Standard Edition, and do not include it on other types of servers (Archive Server, Network Gateway, Curator).

Database packages	Purpose
Oracle Server Extension	Contains the files necessary to build an Oracle Server database to be used by IMPAX. New installs only. Not supported for upgrades.

AS300 installer log files

(Topic number: 6780)

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

Determining a password for the AgfaService account

(Topic number: 7705)

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

- Be at least eight characters long
- Not contain three or more characters from the user's account name
- Contain characters from at least three of the following five categories:
  - Uppercase (A to Z)
  - Lowercase (a to z)
  - Digits (0 to 9)
  - Non-alphanumeric (for example, !, $, #, or %); avoid commas
  - Unicode

Installing hardware and software on an AS300 server

2

Before installing IMPAX on an AS300 server, you must install and configure the required hardware and software components.

If you are using Solaris Database Server (in a mixed-host configuration), instead refer to the "Getting started" and "Setting up a Solaris server" sections of the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

1. Installing and configuring Windows Server 2008

(Topic number: 98105)

Follow these instructions to install and configure Microsoft Windows Server 2008 on new AS300 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.

Adding roles and role services in Windows 2008

(Topic number: 104586)

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

Roles:

- Active Directory Lightweight Directory Services (AD LDS)—needed for all-in-one servers and single-servers only
- Web Services IIS Features

Role services:

Role services other than IIS 6 Management Compatibility are required for all-in-one servers and single-servers only.

- ASP.NET
- Windows Authentication
- IP and Domain Restrictions
- Dynamic Content Compression
- IIS 6 Management Compatibility

To add roles and role services in Windows 2008

1. Open the Windows Administrative Tools and select **Server Manager**.
2. Select **Roles** from the pane on the left.

3. Click **Add Roles**.
4. On the Before you begin page, click **Next**.
5. In the Add Roles wizard, select **Web Services (IIS)**. If installing an all-in-one server or a single server, also select **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 **IIS 6 Management Compatibility** checkbox. If installing an all-in-one or a single server, also select the **IP and Domain Restrictions**, **.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.

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.

Activating Windows Server 2008

(Topic number: 109368)

Windows Server 2008 must initially be activated.

To activate Windows Server 2008

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

Changing the paging file setting

(Topic number: 106540)

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

To change the paging file setting

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

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

Configuring Windows Explorer to show all files

(Topic number: 47547)

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

To configure Windows Explorer to show all files

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

Deleting the hiberfil.sys file in Windows 2008

(Topic number: 118485)

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

To delete the hiberfil.sys file in Windows 2008

1. Open a command prompt.
2. Type

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

Creating a temporary directory

(Topic number: 49277)

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

To create a temporary directory

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

Supporting security certificate validation

(Topic number: 47577)

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

To support security certificate validation

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

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.

2. Partitioning disks

(Topic number: 7032)

To store the files and programs required, create logical volumes as shown in the table in *Recommended disk partitions* (refer to page 33). This procedure assumes that the server has multiple disks. If it has only one disk, create all the logical volumes on the same disk.

Important!

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

Recommended disk partitions

(Topic number: 7056)

When partitioning disks, consider the following:

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

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

You must create subdirectories in the CACHE or WEBCACHE partitions to store the imaging data. The existing SYSTEM volume on C should be used for Windows and all program files. The C drive is 40 GB and is created while installing Microsoft Windows 2008.

Letter	Volume label	Size	Server	Used for
E	DATABASE	73 GB	single-host Database Server	SQL Server or Oracle files and database
F	DATABASELOGS	73 GB	single-host Database Server	Oracle archive logs and backup. (Not required for SQL Server databases.)
G	VOLUMES	10 GB	single-host Archive Server	CD-R or DVD-R images
H	LOGS	1 GB	single-host Archive Server Network Gateway	Log files

Letter	Volume label	Size	Server	Used for
			Curator	
I	CACHE-I or WEBCACHE-I	Remaining space	single-host Archive Server Network Gateway Curator	IMPAX image files Consider labeling partitions on the Curator machine WEBCACHE-I, WEBCACHE-J, and so forth for the Mitra Wavelet images
J *	GHOST	20 GB	single-host Database Server Archive Server Network Gateway	Software repository and Symantec Ghost backup images

* If you have more than one CACHE volume, assign drive letters to the CACHE volumes first, then create the GHOST volume.

Note:

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

Creating logical volumes

(Topic number: 15469)

Creating logical volumes improves system performance.

To create logical volumes

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

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

Screen	Select
Specify Volume Size	
Assign Drive Letter or Path	• Select **Assign the following drive letter**

Screen	Select
Format Partition	• Select **Format this volume with the following settings** • File system: **NTFS** • Allocation unit size: **Default** • Select the **Perform a quick format** checkbox.

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

3. Installing Oracle Server on Windows

(Topic number: 65088)

Important!

This topic applies only to Database and single-host servers.

Before installing Oracle Server, verify that the disk has been partitioned into at least two drives (in addition to the C: drive) with a minimum size of 73 GB each. During the installation, the Oracle Server installer automatically selects the first two drives that meet this requirement; the installation fails if two such drives are not available.

Important!

Before installing Oracle Server, disable all virus protection software.

Oracle is installed separately from the IMPAX AS300 Server software. The Oracle software appears on the Oracle on Windows 32-bit and the Oracle on Windows 64-bit DVDs.

CAUTION!

The **installOracleInfo** file defines certain attributes used by the Oracle installation scripts. We do not recommend changing this file because if the file is corrupted, the Oracle installation fails and the system provides no indication of the problem origin. If this file needs to be modified for any reason, use the Wordpad editor to view the file. After any changes are made, run the **dos2unix** command on the file so that it has the correct line endings.

To install Oracle Server on Windows

1. Insert the Oracle on Windows 32-bit DVD or the Oracle on Windows 64-bit DVD.

Use the DVD appropriate to the version of Windows running on the server. While you can install Oracle for Windows 32-bit on a 64-bit Windows system, we recommend using the 64-bit version to take advantage of the enhanced processing power.

2. From the DVD drive, run **setup.bat**.

   Cygwin is automatically installed before the Oracle installer starts.

3. If the `Install client or server?` prompt appears, type **server**.

   If installing Oracle on Windows 64-bit, this prompt does not appear.

4. At the `enterprise or standard edition?` prompt, do one of the following:

   To install Oracle Standard Edition, press **Enter**.

   or

   To install Oracle Enterprise Edition, type **enterprise**.

5. At the `What machine is repository host? [localhost]` prompt, if it is the localhost, press **Enter**. Otherwise, specify the appropriate IP address.

6. At the `Where is software repository?` prompt, if installing from the DVD drive on F, press **Enter**. Otherwise, type the DVD drive or the software repository directory.

7. At the `Temporary directory is c:/cygwin/tmp?` prompt, press **Enter** to accept the default location. Otherwise, type the directory to use.

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

8. After the `Oracle installation complete` message appears, restart the server.

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

Verifying the Oracle for Windows installation

(Topic number: 65297)

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

To verify the Oracle for Windows installation

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

If you spot the following error in the log file:

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

you can ignore it.

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

4. Backing up an image of the Windows installation

(Topic number: 7136)

Symantec Ghost is used to back up the system at defined intervals in case the system must be restored. The application resides on a separate, bootable CD. We recommend that you create a backup of the Windows installation now.

To back up an image of the Windows installation

1. Follow the manufacturer's instructions for creating a ghost backup.

5. 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**.

6. Installing a modem

(Topic number: 7681)

The modem is an optional component. If necessary, install the external modem according to the manufacturer's instructions.

7. 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.

8. 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.

9. 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**.

10. Obtaining Server license keys

(Topic number: 7637)

IMPAX uses software license keys that are unique to the station on which the software is installed. One license key is required for the Network Gateway and a separate license key must be obtained for the Archive Server (even if using PACS Store and Remember archiving).

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 an IMPAX AS300 single-host server

3

An AS300 single-host server includes the database, archive, Network Gateway, and Curator components all on the same server. Before proceeding with the IMPAX AS300 single-host server installation, ensure that the system has been readied as outlined in *Installing hardware and software on an AS300 server* (refer to page 27).

1. Installing the 32-bit IMPAX 6.5.1 AS300 packages

(Topic number: 7144)

Use the IMPAX installer to install the necessary AS300 packages on the system. These packages are described in *32-bit AS300 installer packages reference* (refer to page 22).

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

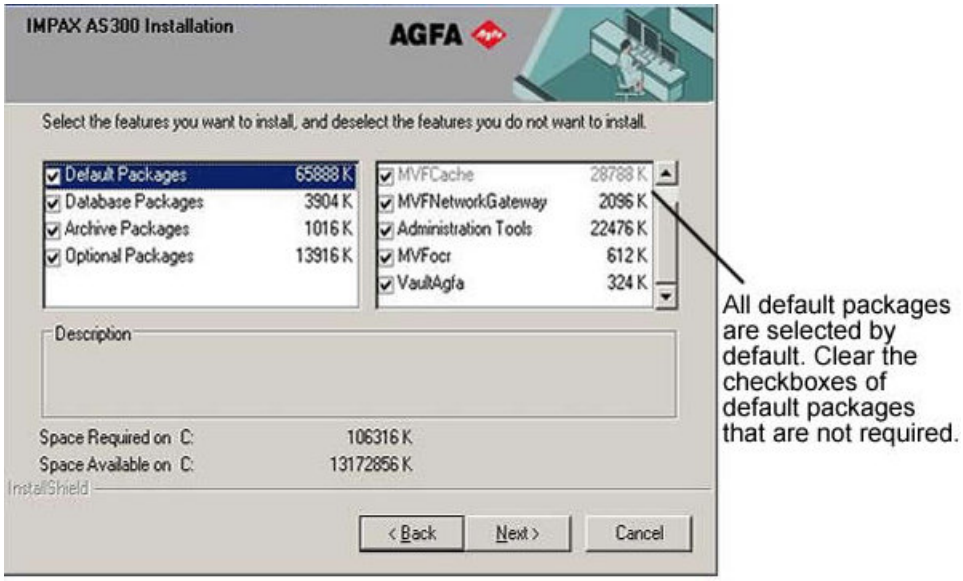
To install the 32-bit IMPAX 6.5.1 AS300 server packages

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

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

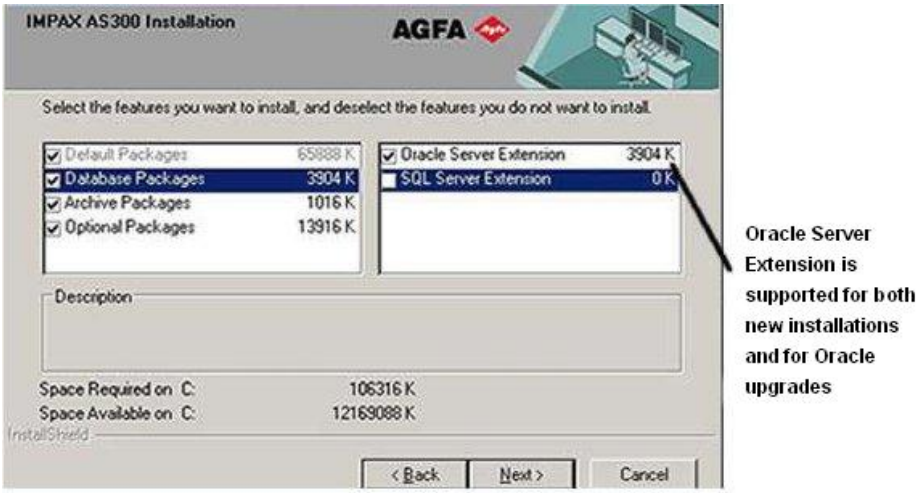
   For a dedicated Database Server, normally clear the **MVFNetworkGateway** and **MVFocr** checkboxes.

For a single-host server, normally all Default Packages are required except, potentially, **MVFocr**.



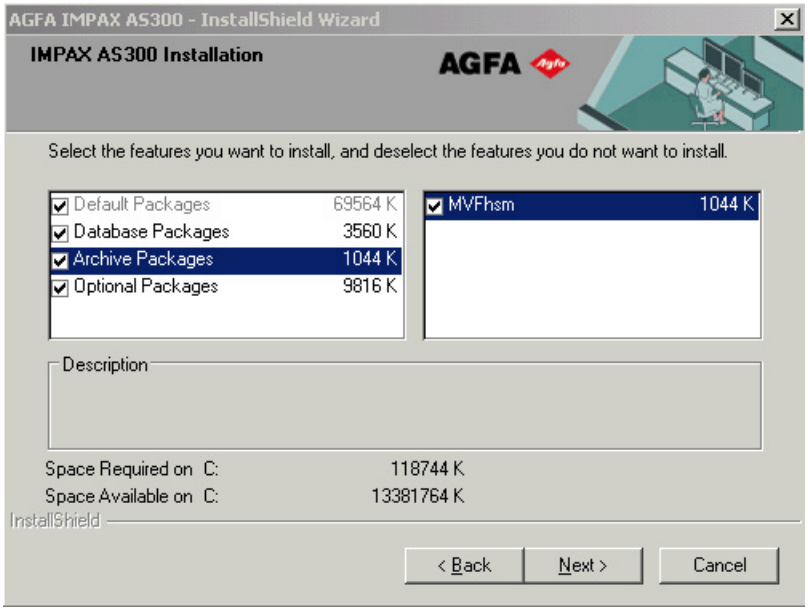
6. Select the **Database Packages** label, then select the appropriate checkbox—normally **Oracle Server Extension**.

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



7. For a dedicated Database Server, clear the **Archive Packages** checkbox.

   For a single-host server, if using HSM archiving, select the **Archive Packages** label, then ensure that the **MVFhsm** checkbox is selected. If using PACS Store and Remember archiving exclusively, or not using the station for archiving at all, clear the **MVFhsm** checkbox.



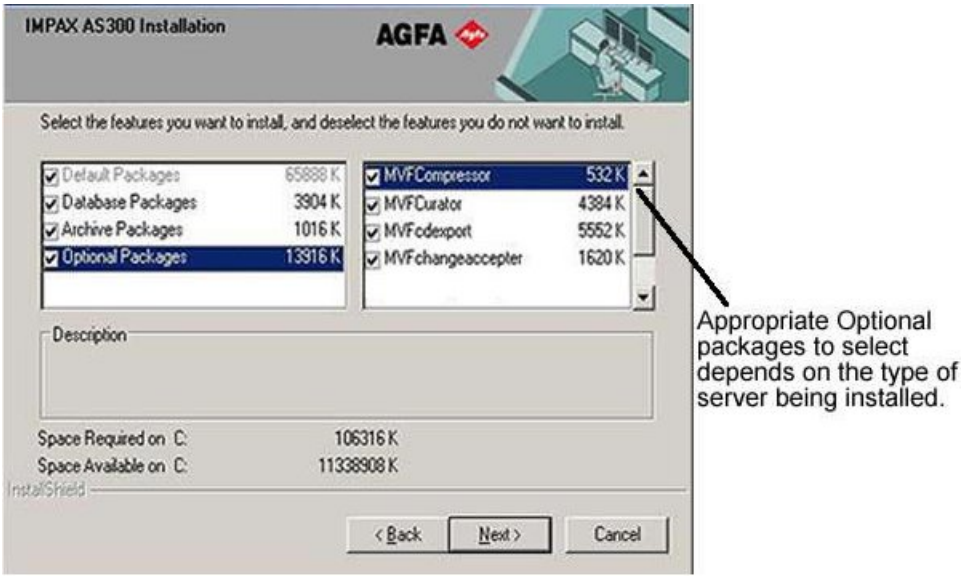
8. Select the **Optional Packages** label, then select the checkboxes of any optional packages that should be installed.

   For a dedicated Database Server, normally clear the checkboxes of all optional packages other than **MVForadg**, if using Oracle Data Guard.

   For a single-host server, you can potentially install all optional packages other than **MVFchangeaccepter** and **MVForadg**.

Note:

Oracle Data Guard is supported only by Oracle Server Enterprise Edition. A single-host server cannot be an Oracle Data Guard server.



9. Click **Next**.
10. For a single-host server, in the MVF License Location dialog, browse to the location of the MVF license file and click **OK**.

    If the mvf.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.
11. For a single-host server, browse to the location of the MVF archive licence file and click **OK**.

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

    The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 26).
13. On the Type of Install screen, select **Create a New Database** and click **Next**.
14. On the confirmation dialog, click **Yes**.
15. If installing the Oracle Server Extension, when prompted, define a Flashback Recovery Area size. Specify a size that is 3 to 5 times the expected size of the database file. Ensure that the drive used for storing Oracle backups has sufficient disk space.

    This area will be used for Oracle database backup and recovery.
16. On the Summary screen, to continue the installation, click **Next**.
17. To display the log file for the database scripts, when prompted, click **Yes**.
18. Check the log files for errors, then close the log files.

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

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

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

2. Confirming that the correct IMPAX AS300 packages are installed

(Topic number: 105679)

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

To confirm that the correct IMPAX AS300 packages are installed

1. Open Control Panel.
2. Select **Programs and Features**.
3. Select **AGFA IMPAX AS300** and click **Change**.

4. After the installer launches, click **Modify**.
5. Click **Next**.
6. Verify that the list of installed packages is correct and remove any if necessary.

   If necessary, uninstall IMPAX 6.5.1 Server and reinstall.

3. Configuring the Enterprise Management console for Oracle 10.2.0.4

(Topic number: 120815)

The Oracle Enterprise Manager is a browser-based GUI through which administrators can perform all monitoring, administration, and configuration tasks for the enterprise. The IMPAX installation scripts install the necessary components to run the Enterprise Management Console on the Oracle 10g server. However, you must configure the service manually.

Note:

If you have problems configuring the Enterprise Management console, refer to the *IMPAX 6.5.1 Server Knowledge Base* topic "Troubleshooting: Cannot configure the Oracle 10.2.0.4 Enterprise Management console" (Topic number 120817).

To configure the Enterprise Management Console for Oracle 10.2.0.4

1. If the Database Server is running on a Solaris system, log into the database server as the **oracle** user.

   or

   Log into the Database Server as the **Administrator** user.
2. Open a sqlplus session.
3. Set the database parameter job queue processes by typing

   alter system set job_queue_processes = 10 scope = BOTH;
4. If Oracle is running on a Windows system, skip ahead to step 8.
5. If Oracle is running on a Solaris system, at the Solaris prompt, change to the /opt/oracle/current/network/admin directory.
6. Create a link for the listener.ora file. If the listener.ora file already exists, remove it prior to creating the link. To create the link, type:

   ln -s /var/opt/oracle/listener.ora listener.ora
7. At the Solaris prompt, verify that the link was created by typing

   lrt

   To the right of the date field, the listener.ora file is listed as:

   ```
   listener.ora -> /var/opt/oracle/listener.ora
   ```

8. Start the configuration assistant by typing

   emca -config dbcontrol db -repos create

   or

   If you are attempting to start the configuration assistant a second time, type

   emca -config dbcontrol db -repos recreate
9. When prompted for the Database SID, type

   MVF
10. When prompted for the listener port number, type

    1521
11. When prompted for the SYS user password, type

    stayout
12. When prompted for the DBSNMP user password, type:

    long2figureout
13. When prompted for the SYSMAN user password, type

    sysman
14. Respond to other prompts appropriately.

Note:

The Email address for notifications and Outgoing Mail (SMTP) server for notifications fields are optional.

15. When the system displays the message `Do you wish to continue? [yes(Y)/no(N)]:`, type

    y
16. Log on to the Enterprise Manager, open a web browser and, in the address bar, type the following address:

    https://*Database_Server name*:1158/em

4. Configuring Windows 2008 to take advantage of available memory

(Topic number: 107414)

Important!

This task is required only on 32-bit Windows systems—not on 64-bit Windows.

On servers with 4 GB of RAM or more, Windows 2008 systems are not configured to take full advantage of Physical Address Extensions (PAE) or Address Windowing Extensions (AWE). This can cause problems, particularly if installing under Oracle for Windows.

To configure Windows 2008 to take advantage of available memory

1. Log into Windows as an administrator-level user.
2. Open a command prompt.
3. Type

   BCDEdit /set PAE ForceEnable

   BCDEdit /set IncreaseUserVA 3072

   If this server is a dedicated Oracle database server, continue with the remaining steps.
4. Restart the system.
5. Log into Windows as the **AgfaService** user.
6. Open a command prompt.
7. Type the following commands:

   sqlplus / sysdba

   alter system set sga_max_size=2776629248 scope=spfile;

   alter system set sga_target=2776629248 scope=spfile;

   exit
8. Open the Windows Administrative Tools and select **Services**.
9. Restart the **OracleServiceMVF** service.

5. 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.

6. Configuring the Audit Record Repository database connection

(Topic number: 32237)

After installing or upgrading the database and adding an Audit Record Repository, you must update certain entries in the database to ensure that auditing functions correctly.

To configure the Audit Record Repository database connection

1. On the IMPAX Database Server, open a command prompt or terminal window.
2. Change to the **C:\mvf\bin** (AS300) or **/usr/mvf/bin** (AS3000, logged in as mvf user) directory.
3. Type **clui**.
4. To check if the entry already exists in the database, type

```
select * from map_ini where ini_key='ARR_INSTALLED' and
ini_section='MAP_EVENT'
```

5. If the entry exists, to update the entry, type

```
update map_ini set ini_value='T' where ini_key='ARR_INSTALLED' and
ini_section='MAP_EVENT'
```

   or if the key does not exist, to insert it, type

```
insert into map_ini (ini_section,ini_key,ini_value) values
('MAP_EVENT','ARR_INSTALLED','T')
```

The Application Server must also be connected to the Audit Record Repository. For details, refer to "Connecting IMPAX Application Server to Audit Manager" (topic number 11444) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Installing a dedicated IMPAX AS300 Database Server

4

A dedicated Database Server contains only the database component of the IMPAX Server, with no archive or Curator. If you have installed a single-host AS300 server, or any configuration of AS3000 Database Server, do not also install a dedicated AS300 Database Server. And before proceeding with the AS300 Database Server installation, ensure the system has been readied as outlined in *Installing hardware and software on an AS300 server* (refer to page 27).

1. Installing a dedicated 64-bit IMPAX AS300 Database Server

(Topic number: 65408)

A dedicated installer exists for installing an IMPAX AS300 Database Server on a 64-bit Windows system. This package cannot be installed on 32-bit Windows systems.

Note:

The AdministrationTools package is not available from the 64-bit installer. Therefore, you must install that package on another AS300 server in the cluster.

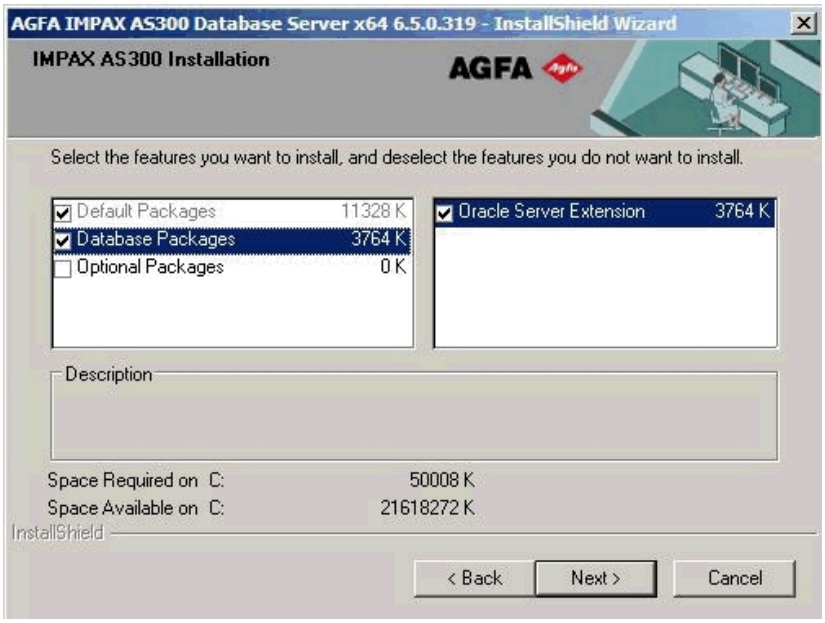
To install IMPAX AS300 Server, you must be logged into Windows as an administrator-level user.

To install a dedicated 64-bit IMPAX AS300 Database Server

1. Insert the IMPAX AS300 DVD.
2. Navigate to **D:\programs\mvf** and double-click **as300-installer-x64.exe**.
3. Type your name (minimum three characters).

This information is recorded in the installer log file.

4. On the Welcome screen, click **Next**.
5. On the Select features screen, the appropriate packages are already selected, so click **Next**.



6. When prompted, type the password for the AgfaService user.

   The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 26).
7. On the Type of Install screen, select **Create a New Database** and click **Next**.
8. On the confirmation dialog, click **Yes**.
9. When prompted, define a Flashback Recovery Area size. Specify a size that is 3 to 5 times the expected size of the database file. Ensure that the drive used for storing Oracle backups has sufficient disk space.

   This area will be used for Oracle database backup and recovery.
10. Type the name of the Application Server and click **Next**.
11. Click **Install**.
12. On the screen displaying the message `Database build is complete. Review the log files to check for any errors`, click **Yes**.

    The build_mvf.log file opens in a text editor.
13. After reviewing the build_mvf.log file, close the file so that the installation can continue.
14. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

2. Installing the 32-bit IMPAX 6.5.1 AS300 packages

(Topic number: 7144)

Use the IMPAX installer to install the necessary AS300 packages on the system. These packages are described in *32-bit AS300 installer packages reference* (refer to page 22).

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

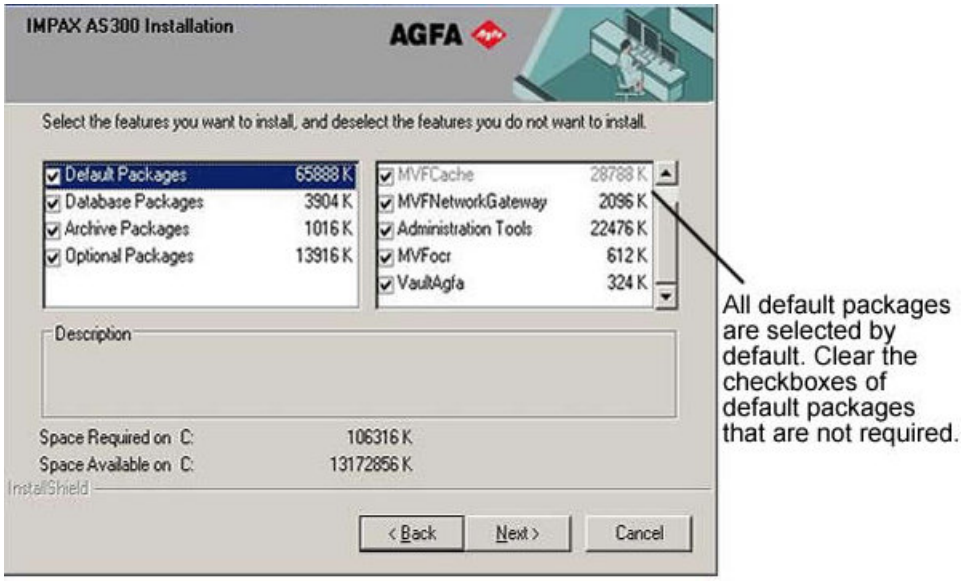
To install the 32-bit IMPAX 6.5.1 AS300 server packages

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

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

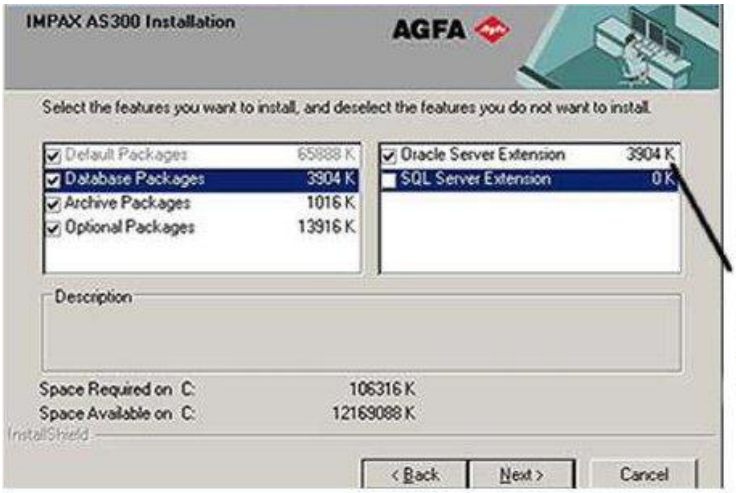
   For a dedicated Database Server, normally clear the **MVFNetworkGateway** and **MVFocr** checkboxes.

   For a single-host server, normally all Default Packages are required except, potentially, **MVFocr**.



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

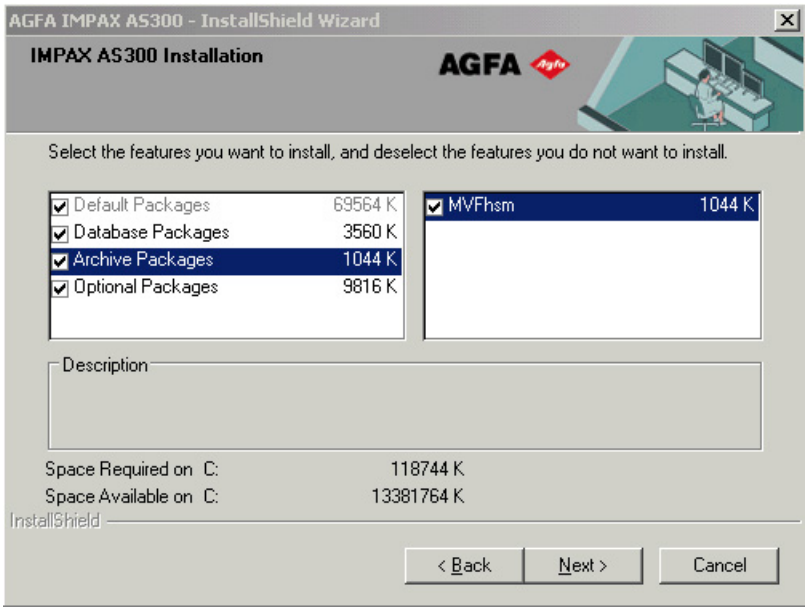
   Oracle Server Extensions are required when using an Oracle database. Oracle is the recommended database for standard new installs.



Oracle Server Extension is supported for both new installations and for Oracle upgrades

7. For a dedicated Database Server, clear the **Archive Packages** checkbox.

   For a single-host server, if using HSM archiving, select the **Archive Packages** label, then ensure that the **MVFhsm** checkbox is selected. If using PACS Store and Remember archiving exclusively, or not using the station for archiving at all, clear the **MVFhsm** checkbox.



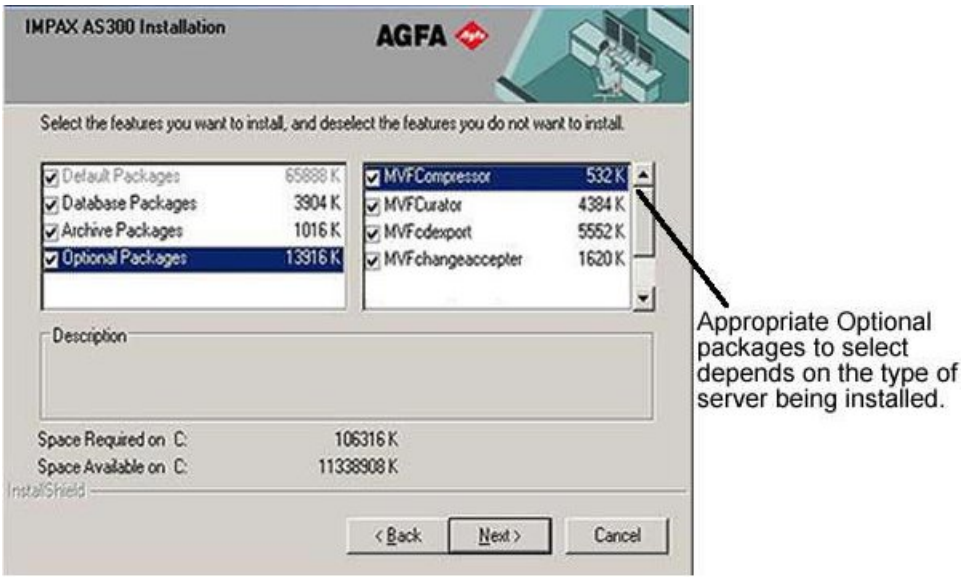
8. Select the **Optional Packages** label, then select the checkboxes of any optional packages that should be installed.

   For a dedicated Database Server, normally clear the checkboxes of all optional packages other than **MVForadg**, if using Oracle Data Guard.

   For a single-host server, you can potentially install all optional packages other than **MVFchangeaccepter** and **MVForadg**.

Note:

Oracle Data Guard is supported only by Oracle Server Enterprise Edition. A single-host server cannot be an Oracle Data Guard server.



9. Click **Next**.
10. For a single-host server, in the MVF License Location dialog, browse to the location of the MVF license file and click **OK**.

    If the mvf.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.
11. For a single-host server, browse to the location of the MVF archive licence file and click **OK**.

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

    The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 26).
13. On the Type of Install screen, select **Create a New Database** and click **Next**.
14. On the confirmation dialog, click **Yes**.
15. If installing the Oracle Server Extension, when prompted, define a Flashback Recovery Area size. Specify a size that is 3 to 5 times the expected size of the database file. Ensure that the drive used for storing Oracle backups has sufficient disk space.

    This area will be used for Oracle database backup and recovery.
16. On the Summary screen, to continue the installation, click **Next**.
17. To display the log file for the database scripts, when prompted, click **Yes**.
18. Check the log files for errors, then close the log files.

The log files must be closed for the installation script to continue.

19. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

3. Configuring the Enterprise Management console for Oracle 10.2.0.4

(Topic number: 120815)

The Oracle Enterprise Manager is a browser-based GUI through which administrators can perform all monitoring, administration, and configuration tasks for the enterprise. The IMPAX installation scripts install the necessary components to run the Enterprise Management Console on the Oracle 10g server. However, you must configure the service manually.

Note:

If you have problems configuring the Enterprise Management console, refer to the *IMPAX 6.5.1 Server Knowledge Base* topic "Troubleshooting: Cannot configure the Oracle 10.2.0.4 Enterprise Management console" (Topic number 120817).

To configure the Enterprise Management Console for Oracle 10.2.0.4

1. If the Database Server is running on a Solaris system, log into the database server as the **oracle** user.

   or

   Log into the Database Server as the **Administrator** user.

2. Open a sqlplus session.
3. Set the database parameter job queue processes by typing

   alter system set job_queue_processes = 10 scope = BOTH;

4. If Oracle is running on a Windows system, skip ahead to step 8.
5. If Oracle is running on a Solaris system, at the Solaris prompt, change to the /opt/oracle/current/network/admin directory.
6. Create a link for the listener.ora file. If the listener.ora file already exists, remove it prior to creating the link. To create the link, type:

   ln -s /var/opt/oracle/listener.ora listener.ora

7. At the Solaris prompt, verify that the link was created by typing

   lrt

   To the right of the date field, the listener.ora file is listed as:

   ```
   listener.ora -> /var/opt/oracle/listener.ora
   ```

8. Start the configuration assistant by typing

   emca -config dbcontrol db -repos create

   or

   If you are attempting to start the configuration assistant a second time, type

   emca -config dbcontrol db -repos recreate

9. When prompted for the Database SID, type

   MVF

10. When prompted for the listener port number, type

    1521

11. When prompted for the SYS user password, type

    stayout

12. When prompted for the DBSNMP user password, type:

    long2figureout

13. When prompted for the SYSMAN user password, type

    sysman

14. Respond to other prompts appropriately.

Note:

The Email address for notifications and Outgoing Mail (SMTP) server for notifications fields are optional.

15. When the system displays the message `Do you wish to continue? [yes(Y)/no(N)]:`, type

    y

16. Log on to the Enterprise Manager, open a web browser and, in the address bar, type the following address:

    https://*Database_Server name*:1158/em

4. Restoring the database and services

(Topic number: 65027)

CAUTION!

This topic applies only if you are upgrading from a single-host configuration to a multi-host configuration. Do **not** perform this task when installing a new IMPAX AS300 Database Server.

After the new Database Server is installed, restore the Oracle backup from the existing single-host server onto this new server.

Recovering with the current control file using RMAN

(Topic number: 67052)

This method applies when using Oracle disk backups.

Restoring files from backup is a first step when recovering a database and can also be performed in other cases, such as when upgrading from a single-host to a multi-host configuration. Disk backups are supported for both AS300 and AS3000 Oracle Database Servers.

With the current control file, you can restore the database to the point of the database failure so that no committed transactions are lost.

To recover with the current control file using RMAN

1. Log in as user **oracle** (Solaris) or **AgfaService** (Windows).

   Log in as **Administrator** user.

2. If the Oracle database is still open, shut it down. Type

   rman target /

   shutdown abort;

3. To start up the database, from the rman prompt, type

   startup mount;

4. To restore the database, type

   restore database;

5. After all the files have been restored, at the rman prompt, type

   recover database;

6. If you see the message `Media recovery complete`, type

   alter database open;

7. Type **exit**.

5. 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.

6. Configuring the Audit Record Repository database connection

(Topic number: 32237)

After installing or upgrading the database and adding an Audit Record Repository, you must update certain entries in the database to ensure that auditing functions correctly.

To configure the Audit Record Repository database connection

1. On the IMPAX Database Server, open a command prompt or terminal window.
2. Change to the **C:\mvf\bin** (AS300) or **/usr/mvf/bin** (AS3000, logged in as mvf user) directory.
3. Type **clui**.
4. To check if the entry already exists in the database, type

   ```
   select * from map_ini where ini_key='ARR_INSTALLED' and
   ini_section='MAP_EVENT'
   ```

5. If the entry exists, to update the entry, type

   ```
   update map_ini set ini_value='T' where ini_key='ARR_INSTALLED' and
   ini_section='MAP_EVENT'
   ```

   or if the key does not exist, to insert it, type

   ```
   insert into map_ini (ini_section,ini_key,ini_value) values
   ('MAP_EVENT','ARR_INSTALLED','T')
   ```

The Application Server must also be connected to the Audit Record Repository. For details, refer to "Connecting IMPAX Application Server to Audit Manager" (topic number 11444) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Installing an IMPAX AS300 Archive Server or Network Gateway

5

You can install dedicated IMPAX Archive Server or Network Gateway stations, or you can combine these components on one station. Before proceeding with the Archive Server or Network Gateway installation, ensure that the system has been readied as outlined in *Installing hardware and software on an AS300 server* (refer to page 27), and that you have installed the dedicated Database Server (refer to page 50).

Note:

AS300 Network Gateways and Archive Servers can be combined with an AS3000 (Solaris) Database Server in a mixed-host configuration. Installation instructions for the AS3000 Database Server are provided in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*. In addition, you must generate a portable password file on the AS3000 Database Server. For further details, consult the appendix *AS3000 portable password file* (refer to page 124).

1. Configuring the database connection

(Topic number: 7073)

If connecting to an Oracle on Windows AS300 database or an Oracle for Solaris AS3000 database, install and configure the Oracle for Client for Windows (refer to page 60).

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.

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.

Note:

The tnsnames entry is not added to the tnsnames.ora file during the Oracle 10g Client installation. This entry is added after installing the IMPAX AS300 or AS3000 package.

2. Installing the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages

(Topic number: 6782)

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

Important!

When upgrading IMPAX AS300 software, you must be logged into Windows with the same administrator-level user account used during installation.

Use the IMPAX installer to install the necessary packages on the system (refer to page 22).

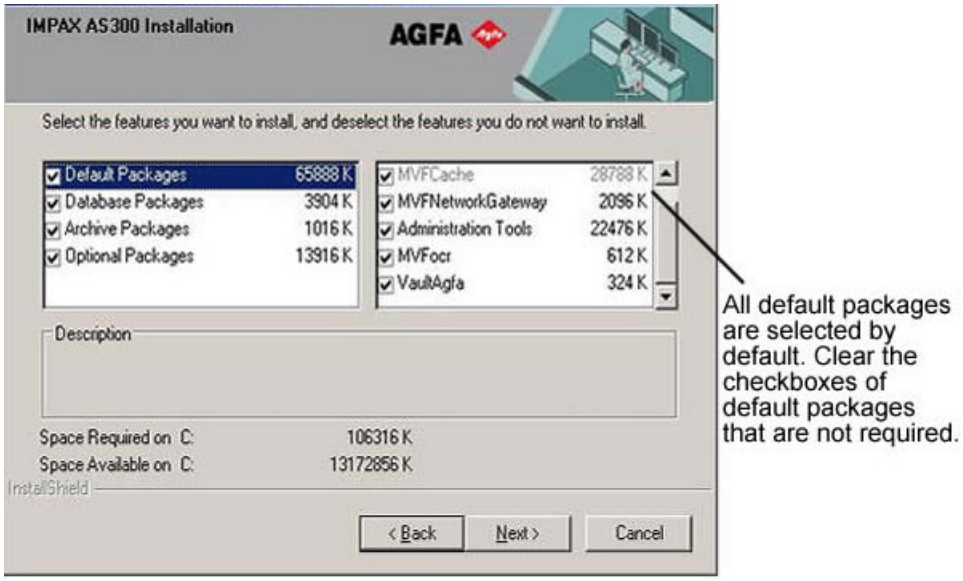
To install the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages

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

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

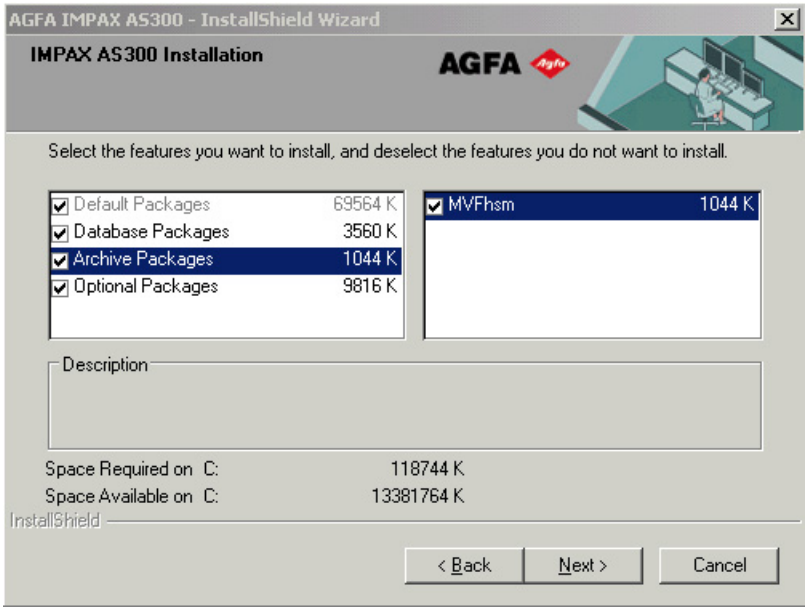
   If installing a Network Gateway or an Archive Server/Network Gateway combination, you can normally leave all the default packages selected.

   If installing a dedicated Archive Server, clear the **MVFNetworkGateway** and **MVFocr** checkboxes.

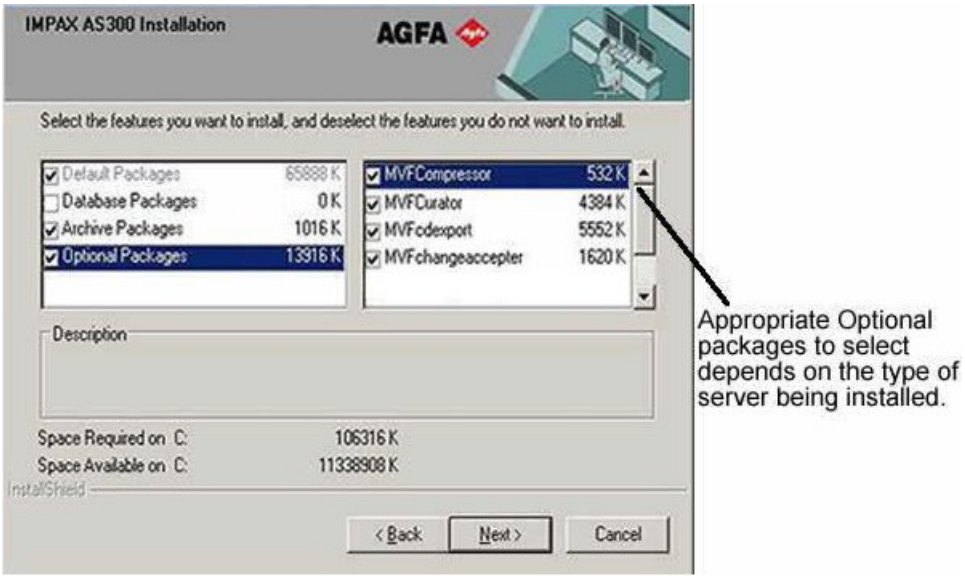


6. Clear the **Database Packages** checkbox.
7. For Archive Servers, select the **Archive Package** label. The MVFhsm is the only archive package listed and is selected by default. If not using an HSM archive, clear the **MVFhsm** checkbox; otherwise, keep it selected.

   For dedicated Network Gateway servers, clear the **Archive Packages** checkbox.



8. Select the **Optional Packages** label.
9. Select any optional packages that should be installed, and clear the other checkboxes.



Unless intending to use this station as a Curator and CD Export server, clear the **MVFCurator** and **MVFcdexport** checkboxes.

MVFCompressor and **MVFPap** may be useful on an Archive Server.

Clear the **MVFchangeaccepter** checkbox.

Do **not** select the **MVForadg** package. This is only for Database Servers using Oracle Data Guard.

10. Click **Next**.
11. If installing a Network Gateway or Archive Server/Network Gateway combination, browse to the location of the MVF license file and click **OK**.

    If the mvf.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.
12. If installing an Archive Server or Archive Server/Network Gateway combination, browse to the location of the MVF archive license file and click **OK**.

    If the mvfarch.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.
13. Browse to the location of the portable password file and click **OK**.
14. Type the temporary password used to create the portable password file and click **Next**.

    The mvf.psd file is imported under C:\mvf.

    Important!

    If the mvf.psd file already exists, do not remove it; otherwise, IMPAX services cannot start.

15. On the Summary screen, click **Next**.

    The files are copied.

16. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

3. Configuring archives

(Topic number: 109244)

An Archive Server consists of a computer with an HSM file system. PACS Store and Remember archiving is also supported. Studies are archived by transmitting them to the Archive Server. The exams are temporarily stored on hard disk (cache) and are eventually stored on long term storage media in the archive. The Archive Server is administered through the Administration Tools.

Each archive type requires special considerations. For example, after the HSM package is installed, a few additional configuration steps are required. For information on configuring archives, refer to "Initially configuring the Archive Server" (Topic number 9177) in the Archive Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

4. Restarting the IMPAX AS300 system

(Topic number: 7113)

Important!

This topic applies only if you are upgrading from a single-host configuration to a multi-host configuration.

Before returning IMPAX to active service, restart the system and ensure that any antivirus services are restarted.

To restart the IMPAX AS300 system

1. Restart the computer.
2. Log into Windows as an administrator-level user.
3. Restart the antivirus software (if stopped).
4. Launch and log into Administration Tools.
5. In Job Manager, restart the halted transmit queues.
6. Restart the halted archive queues.

5. Configuring web cache folder permissions

(Topic number: 7077)

If the Curator web cache is on a Windows folder location, to ensure that the cache is accessible, give the Administrators account and Group account full read, write, and execute permissions on the cache folder.

To configure web cache folder permissions on Windows Server 2003

1. On the Windows 2003 server hosting the cache, open Windows Explorer.
2. Navigate to the location of the cache.
3. Right-click the cache folder and select **Sharing and Security**.
4. Select **Share this folder**.
5. Type an appropriate Share name.
6. Click **Permissions**.
7. Select **Everyone**, then click **Remove**.
8. Click **Add**.
9. In the field for object names, type **Administrators; ImpaxServerGroup**, then click **Check Names**.
10. If the names are not found, click **Advanced**, then click **Find Now**. Select the **Administrators** and **ImpaxServerGroup** accounts and click **OK**.
11. To close the Select Users or Groups dialog, click **OK**.
12. In the Permissions for *share_name* dialog, to give each user full read, write, and execute access to the cache volume folder, select each user and select **Full Control**.
13. Close the permissions and properties dialogs.

To configure web cache folder permissions on Windows Server 2008

1. On the Windows 2008 server hosting the cache, open Windows Explorer.
2. Navigate to the location of the cache.
3. Right-click the cache folder and select **Properties**.
4. Switch to the **Sharing** tab.
5. Click **Advanced Sharing**.
6. Select **Share this folder**.
7. Type an appropriate Share name.
8. Click **Permissions**.
9. Select **Everyone**, then click **Remove**.

10. Click **Add**.
11. In the field for object names, type **Administrators; ImpaxServerUser**, then click **Check Names**.
12. If the names are not found, click **Advanced**, then click **Find Now**. Select the **Administrators** and **ImpaxServerUser** accounts and click **OK**.
13. To close the Select Users or Groups dialog, click **OK**.
14. In the Permissions for *share_name* dialog, to give each user full read, write, and execute access to the cache volume folder, select each user and select **Full Control**.
15. Close the permissions and properties dialogs.

6. Creating a web cache volume

(Topic number: 7069)

You must manually create cache folders on the system. You can then configure the cache volume in Administration Tools on the Database Server.

To create a web cache volume

1. On the Database Server, log into the Administration Tools.
2. Click **Cache Manager**. 
3. Click **New Cache Volume**. 
4. Select **Web Cache**.
5. From the Station list, select the station where the master curator is installed.
6. In the Path field, type the path for the new cache volume.
    - Do not use a trailing slash or backslash at the end of the volume path, because this can create problems when retrieving images from the cache. For example, do not type **\\server\WEBCACHE1**; instead, use **\\server\WEBCACHE1**.
    - All caches on the system (image and web) must be shared. Shared caches are specified without the volume letter; for example, instead of **\\server\f$\CACHE1**, use **\\server\CACHE1**.
7. Click **Add**.
8. In the Warning dialog, verify that the path is correct and click **Yes**.

Completing the installation of an IMPAX AS300 cluster

6

After the installation and preliminary setup of an IMPAX AS300 server, whether in a single-host, multi-host, or mixed-host configuration, additional tasks are required to complete the installation. For more information on how to configure the IMPAX system using the Administration Tools, refer to the Administration Tools component of the IMPAX 6.5.1 Server Knowledge Base.

1. Configuring Data Execution Prevention (DEP)

(Topic number: 7192)

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

Note:

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

To configure Data Execution Prevention (DEP)

1. Right-click **Computer** and select **Properties**.
2. Under Tasks in the left pane, select **Advanced system settings**.
3. If not selected, switch to the **Advanced** tab.

4. Under Performance, click **Settings**.
5. Switch to the **Data Execution Prevention** tab.
6. In the Performance Options dialog, select **Turn on DEP for all programs and services except those I select**.
7. For each IMPAX executable in the list that follows, click **Add**, navigate to C:\mvf\bin, select the executable, and click **Open**:
    a. **curator.exe**
    b. **ddo_create.exe**
    c. **ddo_store.exe**
    d. **mvf_scp.exe**
    e. **mvf_scu.exe**
    f. **mvf_compressor.exe**
    g. **mvf_autopilot.exe**
8. Click **OK** and close all open dialogs.
9. Restart the system.

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

2. Installing Server license keys on a new server

(Topic number: 40455)

If you have not already installed the appropriate license keys on the servers, do so now. MVF license keys must be installed on each single-host and Network Gateway station. Archive license keys must be installed on each single-host and Archive Server station.

If you do not have license keys, you must obtain them from the Agfa Account Manager. More information, including details about obtaining the MAC address, is available in *Obtaining Server license keys* (refer to page 40).

Installing the mvf license key on a Windows server

(Topic number: 40452)

If you have not installed the license key with the software, you can do so afterward by following this procedure.

To install the mvf license key on a Windows server

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

    The license key file name is the MAC address with a .lic file extension.
2. Open Windows Explorer.

3. Copy the license key file to **C:\mvf**.
4. Rename the license key file to **mvf.lic**.

Installing the archive license key on a Windows server

(Topic number: 15609)

Using PACS Store and Remember archiving (or any other type of archiving) requires that an archive license key be installed on the server.

To install the archive license key on a Windows server

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

   The license key file name is the MAC address with a .lic file extension.
2. Open Windows Explorer.
3. Copy the archive license key to the C:\mvf directory.
4. Rename the license key to **mvfarch.lic**.

3. Installing the Application Server

(Topic number: 40165)

Before configuring IMPAX Server, install the Application Server software. Refer to the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

Note:

If installing a single-host AS300 (Windows) server, you can optionally install the Application Server software on that same server, creating what is called an *all-in-one* server.

4. Installing the IMPAX Server documentation

(Topic number: 6962)

The IMPAX Server documentation is located on the IMPAX Documentation DVD. You install it on an IMPAX Application Server, not on any of the AS300 or AS3000 servers. Refer to "Installing the IMPAX documentation" (topic number 15523) in the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide*.

5. Installing and configuring Curator

(Topic number: 7152)

After installing the Application Server and performing its initial configuration, install and configure the Curator server, as per the instructions in the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*.

6. IMPAX services that can write to the LOGS partition

(Topic number: 6573)

When IMPAX was installed, the operational log files location is set to C:\mvf\data\logs. If you have created a separate log file partition as outlined in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*, you may want to update the default logging location to write to that partition.

Note:

The subdirectory must exist before logs are written to that path.

For the Archive Server, the following IMPAX services can be modified to write to the LOGS partition.

Service	Process
DICOM Service Class Provider	SCP
DICOM Service Class User	SCU
DICOM Storage Cache Manager	Autopilot
DICOM Storage Cache Server	SPFTPD
MVF HSM Archive	HSM archive
Mitra System Compressor	Lossy Compressor
Mitra System Task Scheduler	Task Scheduler

For the Network Gateway, the following IMPAX services can be modified to write to the LOGS partition.

Service	Process
DICOM Service Class Provider	SCP
DICOM Service Class User	SCU
DICOM Storage Cache Manager	Autopilot
DICOM Storage Cache Server	SPFTPD

Service	Process
Mitra System Compressor	Lossy Compressor
Mitra System Task Scheduler	Task Scheduler

Note:

Not all services may exist on the server.

Updating the IMPAX Server log file locations

(Topic number: 15612)

Ensure that you have noted or referenced which IMPAX services are to be modified.

To update the IMPAX Server log file locations

1. Open the Windows Administrative Tools.
2. Select **Services**.
3. For each service to be updated:
   a. Right-click the service and select **Properties**.
   b. Under Service status, click **Stop**.
   c. In the Start parameters field, type

      -f *full_path_of_log_file*

      For example, **-f h:\log\mitra.log**.
   d. To restart the service, under Service status, click **Start**.

      You must start the service before exiting the Properties dialog; otherwise, your changes are not saved.
   e. To exit the Properties dialog, click **OK**.

Updating logging for the Administration Tools server

(Topic number: 15615)

A separate procedure is performed for the server running the IMPAX Administration Tools.

To update logging for the Administration Tools server

1. Using a text editor, in C:\mvf\java\etc\jclient.properties, search for the following text and modify the path:

   ```
   logDirectory
   ```

   ```
   logFile
   ```

2. Using a text editor, in C:\mvf\java\etc\jserver.properties, search for the following text and modify the path:

   ```
   mtk.logFile
   ```

   ```
   jmtk.logFile
   ```

   Note:

   Use the forward slash (/) in the path names.

3. To resume services, restart the Administration Tools server.

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

7. 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

8. Initially configuring Oracle for Windows

(Topic number: 65079)

After installing Oracle Server for Windows, the Database Server must be configured for database backup times.

Performing a warm backup of the Oracle database

(Topic number: 66644)

With a warm backup, the database does not have to be shut down. Warm backups are therefore less disruptive than cold backups, in which the database does have to be shut down. Still, try to back up the database during non-peak hours, as the backup process consumes a significant amount of disk I/O resources. Avoid performing a backup at the same as time as other database-intensive programs (for example, prefetching) are being run.

To perform a warm backup of the Oracle database

1. Log into the AS300 Database Server as the **AgfaService** user.
2. In a command prompt, change to the **C:\mvf\bin** directory.

   In a command prompt, change to the **C:\Connectivity-Oracle\mcf\etc** directory.
3. If not already done, run **bash configure_backup**.

4. In the command prompt, type **bash runbackup**.

   The backup may take a significant amount of time.

Automating database backups for Oracle

(Topic number: 8908)

To determine when to run the automated backups, configure a cron job (AS3000) or a Scheduled Task (AS300) to run the backup script, located in /usr/mvf/bin/runbackup (AS3000) or bash C:\mvf\bin\runbackup (AS300).

Note:

Change/schedule the backup for a time when the system is under low load, such as overnight.

9. Identifying remote PACS in IMPAX

(Topic number: 7224)

When installing a new IMPAX 6.5.1 cluster, the database is automatically updated with the details for all Archive Server, Network Gateway, Curator, and CD Export server components within the cluster. These do not have to be configured as stations in Network Management.

By contrast, any PACS systems external to the IMPAX cluster must be added as stations using Network Management in the Administration Tools.

Tip:

To identify an older IMPAX system as a remote PACS, add its Network Gateway.

Follow these instructions for each external PACS that IMPAX 6.5.1 can communicate with.

To identify remote PACS in IMPAX

1. In the Administration Tools, on the Setup tab, click **Network Management**.
2. Click **New**.
3. Type the AE Title, Alias, and Host of the station.
4. Switch to the **Capabilities** tab.
5. Under Station Type, select **PACS**.
6. Select the appropriate permissions for the station and server communication.

   For details, refer to "Defining types of communication between stations and the server" (topic number 9000) in the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*.

7. Clear the **Send/Receive LEI only** checkbox.

> **Note:**
>
> In most cases clearing this setting is preferred; however, some systems may have trouble negotiating compression algorithms and may need the LEI only negotiation. Refer to the documentation that accompanies your external PACS. This setting is ignored for older versions of IMPAX, because the IMPAX systems negotiate with a proprietary dialog.

8. Click **Save**.

For more information on adding stations, refer to the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*.

10. Configuring Windows firewall exceptions

(Topic number: 15509)

The Windows firewall filters and blocks unsolicited incoming network traffic. In some circumstances, you may want to allow programs and services to access to a specific server port that is normally blocked by the Windows firewall.

> **Note:**
>
> To use QStar HSM with IMPAX, open port 160 for UDP messages.

To configure Windows firewall exceptions

1. Open Control Panel.
2. Select **Windows Firewall**.
3. Click **Change settings**.
4. Switch to the **Exceptions** tab.
5. Click **Add Port**.
6. Type the Name and Port number.

> **CAUTION!**
>
> If you click **OK** at this point, the port will be available to all IP addresses. To restrict the port to specific, trusted addresses, continue with the next step.

7. Click **Change scope**.
8. In the Change Scope dialog, click **Custom List**.

9. In the field under Custom List, enter a comma-delimited list of IP addresses to give access to the port.

   Note:

   Do not include spaces between IP addresses.

10. Click **OK**.
11. For any other ports to add, repeat from step 5.
12. When done, to close the Add a Port and Windows Firewall dialogs, click **OK**.

The new firewall rule takes effect immediately. You do not have to restart the server.

11. Configuring IMPAX 6.5.1 stations

(Topic number: 7002)

After all cluster components are installed, you must configure the capabilities for each station in the IMPAX 6.5.1 Administration Tools. For details and instructions, refer to the Network Management section (topic number 8988) of the Administration Tools component of the *IMPAX 6.5.1 Server Knowledge Base*. For instructions on installing IMPAX Client, refer to the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide*.

12. Configuring web cache folder permissions

(Topic number: 7077)

If the Curator web cache is on a Windows folder location, to ensure that the cache is accessible, give the Administrators account and Group account full read, write, and execute permissions on the cache folder.

To configure web cache folder permissions on Windows Server 2003

1. On the Windows 2003 server hosting the cache, open Windows Explorer.
2. Navigate to the location of the cache.
3. Right-click the cache folder and select **Sharing and Security**.
4. Select **Share this folder**.
5. Type an appropriate Share name.
6. Click **Permissions**.
7. Select **Everyone**, then click **Remove**.
8. Click **Add**.

9. In the field for object names, type **Administrators; ImpaxServerGroup**, then click **Check Names**.
10. If the names are not found, click **Advanced**, then click **Find Now**. Select the **Administrators** and **ImpaxServerGroup** accounts and click **OK**.
11. To close the Select Users or Groups dialog, click **OK**.
12. In the Permissions for *share_name* dialog, to give each user full read, write, and execute access to the cache volume folder, select each user and select **Full Control**.
13. Close the permissions and properties dialogs.

To configure web cache folder permissions on Windows Server 2008

1. On the Windows 2008 server hosting the cache, open Windows Explorer.
2. Navigate to the location of the cache.
3. Right-click the cache folder and select **Properties**.
4. Switch to the **Sharing** tab.
5. Click **Advanced Sharing**.
6. Select **Share this folder**.
7. Type an appropriate Share name.
8. Click **Permissions**.
9. Select **Everyone**, then click **Remove**.
10. Click **Add**.
11. In the field for object names, type **Administrators; ImpaxServerUser**, then click **Check Names**.
12. If the names are not found, click **Advanced**, then click **Find Now**. Select the **Administrators** and **ImpaxServerUser** accounts and click **OK**.
13. To close the Select Users or Groups dialog, click **OK**.
14. In the Permissions for *share_name* dialog, to give each user full read, write, and execute access to the cache volume folder, select each user and select **Full Control**.
15. Close the permissions and properties dialogs.

13. Creating a web cache volume

(Topic number: 7069)

You must manually create cache folders on the system. You can then configure the cache volume in Administration Tools on the Database Server.

To create a web cache volume

1. On the Database Server, log into the Administration Tools.

2. Click **Cache Manager**. 
3. Click **New Cache Volume**. 
4. Select **Web Cache**.
5. From the Station list, select the station where the master curator is installed.
6. In the Path field, type the path for the new cache volume.
    - Do not use a trailing slash or backslash at the end of the volume path, because this can create problems when retrieving images from the cache. For example, do not type **\\server\WEBCACHE1**; instead, use **\\server\WEBCACHE1**.
    - All caches on the system (image and web) must be shared. Shared caches are specified without the volume letter; for example, instead of **\\server\f$\CACHE1**, use **\\server\CACHE1**.
7. Click **Add**.
8. In the Warning dialog, verify that the path is correct and click **Yes**.

Preparing to upgrade from a single-host to multi-host configuration

7

You must perform certain pre-upgrade steps before upgrading from a single-host configuration to a multi-host configuration.

This workflow assumes that the a new, more powerful server is being deployed to act as the dedicated Database Server. To take advantage of the new processing power, you install the IMPAX AS300 database software on a new server, restore the existing database on that server, then convert the old single-host server into an Archive Server.

1. Upgrading IMPAX from an AS300 single-host configuration to an AS300 multi-host configuration

(Topic number: 7085)

To realize greater workflow volume and enhanced system performance, you may decide to upgrade your IMPAX system from a single-host to multi-host configuration. Perform the database backup, the installs, and the uninstalls in the order listed in the tables that follow.

Prepare the existing single-host server for conversion

☑	Action
	Check the log files and correct any problems noted (refer to page 83)
	Launch Administration Tools and stop the transmit queue (refer to page 83)
	Verify, then archive any unarchived studies (refer to page 84)

☑	Action
	Close all primary archive volumes
	Using Administration Tools, empty the jobs in queues (refer to page 85)
	Halt the archive queue (refer to page 85)
	If not restoring files in the cache directory after the upgrade, remove all database references to images in cache (refer to page 86)
	Stop the antivirus software (refer to page 86)
	Perform an Oracle database check (refer to page 87)
	Back up the database (refer to page 87)
	Copy the system configuration information to a network drive (refer to page 87)
	Stop and remove the MVF services (refer to page 88)

Install the appropriate software on the new server

☑	Action
	Perform the actions listed in *Installing hardware and software on an AS300 server* (refer to page 27)
	Install the IMPAX packages appropriate to a dedicated Database Server—either the 64-bit packages (refer to page 50) or the 32-bit packages (refer to page 52)
	Restore the backed-up database data onto this server (refer to page 57)
	Generate the portable password file (refer to page 57)
	If using an Audit Record Repository, update certain database settings for it (refer to page 58)
	Enable Data Execution Prevention (DEP) (refer to page 67) for all programs and services

Convert the original server into an Archive Server

☑	Action
	Uninstall the IMPAX database, network gateway, and curator packages (refer to page 88)
	Uninstall the Oracle Server software (refer to page 89)
	Disable IIS (refer to page 90)
	Enable autoplay (refer to page 90), if necessary
	Restart the server and services (refer to page 64)

Set up new Network Gateway and Curator servers

	Action
	For the new Network Gateway server, perform the actions listed in *Installing hardware and software on an AS300 server* (refer to page 27)
	For the new Network Gateway, obtain license keys (refer to page 40) by emailing Agfa the server MAC address
	Install IMPAX packages appropriate to a Network Gateway (refer to page 61)
	Restart the server and services (refer to page 64)
	Enable Data Execution Prevention (DEP) (refer to page 67) for all programs and services
	Install and configure the new Curator (refer to page 70)

2. Performing the pre-upgrade check

(Topic number: 7120)

To ensure that any abnormalities in the system are not moved forward with the upgrade, before proceeding with the upgrade, examine the log files for abnormal behavior that may require intervention. The log files are located in C:\mvf\data\logs.

3. Stopping the transmit queue

(Topic number: 7101)

Allow remaining jobs to continue until they have finished, then prevent any more jobs from being processed.

Tip:

Jobs in progress cannot be deleted.

To stop the transmit queue

1. Launch the Administration Tools and log in as user **service**.
2. On the Daily tab, click **Job Manager**.
3. Monitor each Transmit queue and wait for all outgoing jobs to finish.
4. Select each Transmit queue and click **Halt Queue**.
5. To confirm that you want to halt the queue, click **Yes**.

4. Archiving remaining unarchived studies

(Topic number: 7742)

Important!

This topic applies only to an Archive Server or to the Archive component of a single-host server (including standalone with archive and single-server configurations).

Before performing the upgrade, identify remaining unarchived studies. You must store these studies to the archive.

Verifying unverified studies

(Topic number: 60054)

Before archiving studies, verify all unverified studies.

To verify unverified studies

1. In the Administration Tools, on the Daily tab, click **Study Manager**.
2. From the location list, select **Failed Verification**.
3. Set other search criteria to **Any** value.
4. Click **Refresh**.
5. In the search results, select all studies.
6. To fix up the studies that have failed HIS verification, click **Fix All Studies**.
7. Review the results presented in the dialog.

Storing unarchived studies

(Topic number: 60051)

When no studies are returned by the Failed verification query, archive all remaining studies.

To store unarchived studies

1. In the Administration Tools, on the Daily tab, click **Study Manager**.
2. From the location list, select **Cached** (or another value that will return the unarchived studies).
3. Set other search criteria to **Any** value (or set to appropriate values).
4. Click **Refresh**.
5. In the search results, select the studies to archive.

The Location column on the results list shows the current location of the study, and indicates which studies are only in cache (C for system cache, L for local station cache, W for web cache) and not also in an archive location (such as P for PACS archive).

6. Click **Store to Archive**.
7. To update the status of the selected studies, click **Refresh**.
8. Ensure that all studies are archived.

5. Emptying all queues

(Topic number: 40184)

Monitor the Job Manager to make sure that all the queues are empty and that all jobs are completed prior to the upgrade.

To empty all queues

1. In the Administration Tools, on the Daily tab, select **Job Manager**.
2. If an archive job remains in any of the queues, select the job and click **Expedite Selected Job(s)**.
3. If any other job remains in any of the queues, select the job and click **Delete Selected Job(s)**.

6. Halting the archive queue

(Topic number: 40187)

When all archive jobs have been successfully handled, halt the Archive queue to stop studies from moving around the system.

To halt the archive queue

1. In the Administration Tools, on the Daily tab, select **Job Manager**.
2. In the queue list, select the archive queue.
3. Click **Halt Queue**.
4. To confirm that you want to halt the queue, click **Yes**.

7. Deleting cache locations for studies

(Topic number: 7707)

If you are not restoring the files in the cache directory after the upgrade, to prevent database inconsistencies, remove all database references to images in cache.

To remove references to images in cache, find all study_refs that are in the cache and delete them.

Note:

Images in the cache are archived and, if necessary, can be retrieved after the upgrade is complete.

To delete cache locations for studies

1. On a station with a cache containing database references to remove, log in as mvf user and launch CLUI and type the following:

   cache query

   A list of caches and their volume_refs is displayed.

2. To store all study_refs into variable *a*, type

   save_refs a select distinct ds.study_ref from dosr_study ds, dosr_object do where ds.study_ref = do.study_ref and do.object_ref in (select object_ref from osr_location where volume_ref = *volume_ref*)

   where *volume_ref* is the volume reference of the cache.

3. To enter menu mode, type

   Go menu

4. Select **Study Manager**.
5. Select **Delete Studies Menu**.
6. Select **Delete Study from Cache**.
7. To process the study_refs stored in the variable *a*, at the command prompt, type **a**.

   All studies in the volume_ref's cache are removed.

8. Repeat this process on each station in the cluster that has a cache and whose database references you want to remove.

8. Stopping antivirus software

(Topic number: 7616)

If you have antivirus software installed on any Windows-based servers, ensure that no scan jobs are running that would interfere with the upgrade process. Stop the antivirus services.

To stop antivirus software

1. On a Windows server to upgrade, launch the antivirus software.
2. Halt the scan operation according to the vendor's instructions.

9. Checking the Oracle database

(Topic number: 65094)

Check the Oracle database to ensure that no errors are present.

To check the Oracle database

1. Log into the Database Server as the **AgfaService** user.
2. Open a command prompt.
3. Type

   rman target /
4. At the RMAN prompt, type

   backup validate check logical database;
5. Check the results to ensure that no errors appear.

10. Backing up the database

(Topic number: 40171)

Before upgrading the system, create a manual backup of the database. For details on how to do this with an Oracle database, refer to "Manually backing up the Oracle database" (topic number 8900) in the Oracle Server component of the *IMPAX 6.5.1 Server Knowledge Base*. For details on how to do this with a SQL Server database, refer to "Manually backing up the SQL 2005 database" (topic number 7635) in the SQL Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

11. Saving system configuration information

(Topic number: 7109)

Save the system configuration to a safe location on the network.

To save the system configuration information

1. Open a command prompt.
2. To save the IP configuration and ethernet adaptor information to the network location, type:

   ipconfig /all > *drive_letter*:ipconfig.txt

where *drive_letter* is the drive where the ipconfig.txt file resides.

3. To save the host name information to the network location, type:

   hostname > *drive_letter*:hostname.txt

   where *drive_letter* is the drive where the hostname.txt file resides.
4. Copy the hosts file located in C:\WINNT\system32\drivers\etc to the network location.
5. Copy the mvf.lic and mvfarchive.lic files to the network location.

12. Disabling the server

(Topic number: 7180)

To complete the pre-upgrade procedures, disconnect the server from the network and stop and remove the mvf services.

To disable the server

1. Disconnect the server from the network.
2. Browse to C:\mvf\bin\ and run **stopall.bat**.
3. To remove the mvf services, run **removeall.bat**.

13. Uninstalling and disabling software on the original server

(Topic number: 7089)

Finally, on the original server, uninstall the IMPAX packages and SQL Server, and disable the associated services.

Uninstalling IMPAX AS300 server packages

(Topic number: 7090)

On the original server, uninstall the database, Network Gateway, and Curator packages, leaving on the archive packages.

To uninstall the IMPAX AS300 server packages

1. Open Control Panel.
2. Select **Programs and Features**.
3. Select **AGFA IMPAX AS300**.
4. Click **Change**.

5. At the prompt, type your name and click **Next**.
6. On the Welcome screen, select **Modify**. Click **Next**.
7. **Clear** the checkboxes of the following packages, if they are currently selected:
    a. **MVFNetworkGateway**
    b. **MVFOcr**
    c. **Oracle Server Extension**
    d. **MVFCurator**
    e. **MVFcdexport**
    f. **MVForadg**
8. Click **Next**.
9. In the confirmation dialog, click **OK**.
10. On the Maintenance Complete screen, select **No, I will restart my computer later** and click **Finish**.

Uninstalling Oracle on Windows

(Topic number: 65064)

To convert from a single-host server to an Archive Server, the Oracle Database Server must be uninstalled and all of its components removed from Windows.

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 uninstall Oracle on Windows

1. Delete the MVF, or mvf_ora, System Data Source Name (DSN).
2. Select **Start** > **Oracle - ohome** > **Oracle Installation Products** > **Universal Installer**.
3. Click **Deinstall Products**.
4. Select **ohome** and click **Remove**.
5. Confirm the removal by clicking **Yes**.
6. When the uninstall is complete, to exit out of the Oracle Universal Installer, click **Close**, then **Cancel**.
7. Reboot the server.
8. If the Distributed Transaction Coordinator Service is running, stop it.

    Perform this step in the Windows Administrative Tools > Services.
9. If the following directories exist, delete them.

C:\oracle

C:\Program Files\Oracle

C:\OracleDatabase (keep only if reinstalling the same version of oracle)

10. Run regedit and delete the **HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE** key.
11. Delete all files in the C:\cygwin\tmp directory.
12. Delete all files in C:\cygwin\var\tmp directory.
13. Delete the **C:\installOracleInfo** file.
14. Restart the server.

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

You can now install Oracle Client for Windows (refer to page 60) on this server.

Disabling IIS

(Topic number: 15624)

Disable IIS on the original single-host database server so it does not interfere with the upgrade process.

To disable IIS

1. Open the Windows Administrative Tools and select **Services**.
2. In the Services dialog, right-click **FTP Publishing Service**.
3. Select **Properties**.
4. Click **Stop**.
5. From the Startup type list, select **Disabled**.
6. Click **Apply**.
7. Click **OK**.
8. Repeat steps 2 to 7 for the **IIS Admin Service** and **World Wide Web Publishing Service**.

Enabling auto play

(Topic number: 15627)

Autoplay should be enabled by default. However, if it is not, you must enable it to avoid problems between IMPAX and archive devices.

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 enable auto play

1. Select **Start** > **Run**.
2. In the Open field, type **regedit** and click **OK**.
3. In the Registry Editor dialog, expand **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** and select **Cdrom**.
4. Ensure that the value of AutoRun is 1. If it is not, change the value to **1**.
5. Close the Registry Editor dialog.
6. To run the Group Policy Management Console, select **Start** > **Run**.
7. In the Open field, type **gpedit.msc** and click **OK**.
8. In the Group Policy dialog, expand **Computer Configuration** > **Administrative Templates**.
9. Click **System**.
10. Double-click **Turn off Autoplay**.
11. Ensure that the **Not Configured** option is selected.
12. Close the Group Policy dialog.
13. If you made any changes in the registry or Group Management Console, restart the computer and log back in as an administrator-level user.

14. Continuing the upgrade

(Topic number: 7187)

You can now proceed to install the hardware and software on the new Database Server (refer to page 27).

Silent AS300 installation

A

Silent installations are performed when a mass server deployment is necessary - where the installation process is made easier by automation.

Performing a silent AS300 installation

(Topic number: 106330)

If you are installing a database server, make sure Oracle on Windows has been installed before proceeding with the silent AS300 installation.

To perform a silent AS300 installation

1. Consult the table at the end of this topic to select the answer file to use for the type of installation you want to perform.

   Note:

   When using the answer files, the installer program searches for licenses and portable password files in C:\

2. Navigate to the answer file on the AS300 DVD. All answer files can be found under programs\mvf\answer.
3. Use a text editor to update the answer file with the following information

   For database server installations

   - AgfaService password (only if installing a database server). In the text editor, search for both instances of `replace_with_AgfaService_password` and replace the string with the password that should be used.

- Application Server host name (only if installing a database server). In the text editor, search for `app_server_name` and replace the string with the Application Server host name.

For non-database server installations

- Portable Password File Key (only if installing a non-database server). In the text editor, search for `replace_with_portable_psd_password` and replace the string with the key of the portable password file.

4. Open a command prompt.
5. Start the silent installation script by typing

   as300-installer.exe -s -a -s -f *fully_qualified_path_of_answer_file*

The following table contains the names of the answer files included on the AS300 DVD, and the components that are installed

Answer file	Oracle Database	Network Gateway	HSM	Compressor	Curator	CD Export
AS300_CUR_CD.iss					x	x
AS300_HSM.iss			x			
AS300_NWG.iss		x				
AS300_NWG_CUR.iss		x			x	x
AS300_NWG_CUR_JPEG.iss				x	x	x
AS300_ORA64.iss	Oracle 64-bit (requires Windows 64-bit)					
AS300_ORA_NWG_CUR_HSM_JPEG.iss	Oracle	x	x	x	x	x
AS300_ORA_SingleServer_noHSM.iss	Oracle	x				x

Oracle Data Guard: Disaster recovery solution

B

Oracle Data Guard enables and automates the management of a disaster recovery solution for Oracle databases.

What is Oracle Data Guard?

(Topic number: 65374)

Oracle Data Guard enables and automates the management of a disaster recovery solution for Oracle databases.

In an Oracle Data Guard configuration, two database servers run at the same time. The active one is called the *primary database*. The second one is called the *standby database*. As transactions occur in the primary database, redo data is generated and is written to the local redo logs. Data Guard automatically transfers this redo data to the standby sites and applies it to the standby databases, synchronizing them with the primary database. If a problem occurs with the primary database, the standby database can take over as the active database, so the problem on the primary database can be resolved without the site losing access to data.

Oracle Data Guard can be used only with Oracle Enterprise Edition, and not with Oracle Standard Edition. Data Guard can be configured such that backups do not take place, yet the system does not issue an error message. Agfa provides tools to make the configuration and maintenance easier:

1. A set of scripts to automate the configuration of the Data Guard portion of the Oracle database.
2. Implementation of Oracle RMAN (Recovery Manager) to perform a daily backup of the existing database once the configuration has been completed. (Note that RMAN can also be used for backup and recovery exclusive of Oracle Data Guard.)

   We recommend three times the database size for backup allocation.

3. A set of tools to monitor the configuration (refer to page 117).

To use Oracle Data Guard, the IMPAXoradg package (AS3000) or MVForadg package (AS300) must be installed; see *Installing the Oracle Data Guard package on a Database Server* (refer to page 96).

Configuring Oracle Data Guard

(Topic number: 65856)

Data Guard is Oracle's high-availability solution, using primary and standby database servers. For this solution to work, you must configure it correctly.

Oracle Data Guard configuration overview

(Topic number: 66674)

Oracle Data Guard is Oracle's high-availability solution. In an Oracle Data Guard configuration, two database servers run at the same time. The active one is called the primary database. The second one is called the standby database.

The main tasks in setting up an Oracle Data Guard configuration are as follows.

1. Install the IMPAX Database Server following the procedures in the appropriate installation guide: *IMPAX 6.5.1 AS300 Installation and Configuration Guide* or *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

   This will be the primary database.

2. On AS3000 machines, install the IMPAXoradg package as described in *Installing the Oracle Data Guard package on a Database Server* (refer to page 96). When installing an AS300, select the optional MVForadg component.

3. Back up the database on the primary database, then restore it onto the standby server, using one of the following methods:

   - RMAN backup and restore (refer to page 96)

     or

   - Cold backup and restore (refer to page 100)

   This initially configures the standby server.

4. To ensure that the database servers are backed up and that any archive logs no longer required are cleaned up, configure RMAN backups (refer to page 105) on the primary and standby servers.

Installing the Oracle Data Guard package on a Database Server

(Topic number: 66583)

To use Oracle Data Guard, the IMPAXoradg package (AS3000), or the MVForadg package (AS300) must be installed. On the IMPAX AS3000, you must install the IMPAXoradg package separately.

To install the IMPAXoradg package on an AS3000 Database Server

1. Log into the Database Server as the **root** user.
2. Change to the IMPAX software repository directory.
3. Change to the **IMPAX_R6.5-*impax_build_label*** directory.
4. Run the following command:

   pkgadd -d ./IMPAXoradg.pkg

To install the MVForadg package on an AS300 Database Server

1. When installing the AS300, select the MVForadg as one of the optional packages.

Note:

If you did not install MVForadg at installation time, re-run the IMPAX software installer and select the MVForadg package. Installation instructions are available in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide.*

Configuring Oracle Data Guard using RMAN

(Topic number: 125069)

To configure Oracle Data Guard, you must back up the primary database and restore it onto the standby database server. You can do this either by using RMAN, as described in this topic, or through a cold backup and restore (refer to page 100). Large sites may find the cold backup and restore approach is faster than using RMAN.

Note:

We recommend three times the database size for backup allocation.

The following tasks must be performed:

1. Stop IMPAX and the Application Server.
2. Run the Oracle Data Guard configuration on the primary server and start the public listener (refer to page 97).
3. For Solaris servers only: Share the Flashback area.

4. Run the Oracle Data Guard configuration on the standby server (refer to page 98).
5. Complete the Data Guard configuration on the primary server (refer to page 99).
6. Start IMPAX and the Application Server.

Running the Oracle Data Guard configuration on the primary server

(Topic number: 125049)

When backing up and restoring the primary database using RMAN, you must first run the Oracle Data Guard configuration on the primary server.

To run the Oracle Data Guard configuration on the primary server

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.
2. If on Solaris, log in as the **root** user.
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
5. Enter the following information when prompted:
   a. The location of the Flashback partition.

      The location is typically **/flashback** (Solaris) or **E:\data\flashback** (Windows).
   b. Whether the current server is the primary or standby server.
   c. The host names of both the primary and standby server.
   d. The size of the Flash Recovery Area in GB.

      Use a value as prescribed for the /flashback area by the Database Configurator tool. Do *not* include the space for the backups in this amount if backups are on their own file system. Normally, no more than two times the database size is required if backups are separated.
6. When asked if you want to continue with the RMAN backup, type **"y"**.
7. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory.
8. On Solaris, log in as the **oracle** user and type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

mv PWDMVF.ora PWDMVF.ora.pre_dg

orapwd file=PWDMVF.ora password=stayout entries=40

This creates an Oracle password file.

9. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, in a command prompt, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

After the Data Guard configuration is run on the primary server, the public listener needs to be started.

To start the public listener

1. Log in as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Type **lsnrctl start listener_public**.

Next, if using Solaris servers, share the Flashback area; otherwise go directly to restoring the database on the standby server (refer to page 98).

Restoring the database on the standby server

(Topic number: 125059)

Restoring the database on the standby server is required for both Solaris and Windows servers.

To restore the database on the standby server

1. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory
3. On Solaris, type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

   orapwd file=PWDMVF.ora password=stayout entries=40

   This creates an Oracle password file.

4. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

5. On Solaris, to mount the partition locally, log in as the **root** user and type

mount ***primary_server_name:path_to_flashback_recovery_area_on_primary_server*** **/mnt1**

Note:

If the database volumes are mounted using NFS, complete this procedure from the NAS hosting the NFS share to the primary server.

6. Copy all flashback recovery files from the primary server to the standby server.

   On Solaris, change to the mnt1 directory and use the **cp -rp** * **/complete_path_to_standby_database_flashback_area/** command.

   On Windows, use standard file copy and paste functionality.

7. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
8. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.

9. Enter the Flashback and host name information as prompted.
10. When asked if you want to do the RMAN restore, type **"y"**.

Finally, to link the two servers, complete the Data Guard configuration (refer to page 99).

Completing the Data Guard configuration

(Topic number: 125469)

Linking the two servers, a final Oracle Data Guard configuration task is necessary.

To complete the Data Guard configuration

1. Log into the primary server as the **root** (Solaris) or **AgfaService** (Windows) user.
2. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
3. To continue the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.

4. At the prompt, `About to enable log_archive_dest_1 on Primary. Has Data Guard been configured on the Standby?`, type **yes**.
5. When prompted, manually copy the **tnsnames.ora.client** file to the Oracle Client stations.

6. For AS3000 Oracle Clients, also copy the **/usr/mvf/odbc32v52/odbc.ini** file.
7. To free up disk space, clean up the RMAN backup created by the Data Guard configuration by typing:

   rman target /

   delete backup;

Next you must configure RMAN backups (refer to page 105) on the primary and standby servers.

Configuring Oracle Data Guard using cold backup

(Topic number: 124225)

In configuring Oracle Data Guard, the second task is to back up and restore the primary database. You can do this either by using RMAN (refer to page 96) or through a cold backup and restore, as described in the following topics. Large sites may find the cold backup and restore approach is faster than using RMAN.

Note:

We recommend three times the database size for backup allocation.

The following tasks must be performed:

1. Run the Oracle Data Guard configuration on the primary server (refer to page 100).
2. Start the public listener (refer to page 101).
3. Run the Oracle Data Guard configuration on the standby server (refer to page 101).
4. For Solaris servers only: Share the primary Flashback and database areas.
5. Restore the database on the standby server (refer to page 102).
6. Complete the Data Guard configuration by linking the two servers (refer to page 105).

Running the Oracle Data Guard configuration on the primary server

(Topic number: 124026)

When backing up and restoring the primary database through a cold backup and restore, you must first run the Oracle Data Guard configuration on the primary server.

To run the Oracle Data Guard configuration on the primary server

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.
2. If on Solaris, log in as the **root** user.
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To start the Oracle Data Guard configuration:

   On Solaris, type **./setup_dg**.

On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

On Windows, type **bash setup_dg**.

5. Enter the following information when prompted:
   a. The location of the Flashback partition.

      The location is typically **/flashback** (Solaris) or **E:\data\flashback** (Windows).

   b. Whether the current server is the primary or standby server.

   c. The host names of both the primary and standby server.

   d. The size of the Flash Recovery Area in GB.

      Use a value as prescribed for the /flashback area by the Database Configurator tool. Do *not* include the space for the backups in this amount if backups are on their own file system. Normally, no more than two times the database size is required if backups are separated.

6. When asked if you want to continue with the RMAN backup, type **"n"**.
7. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory.
8. On Solaris, log in as the **oracle** user and type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

   orapwd file=PWDMVF.ora password=stayout entries=40

   This creates an Oracle password file.

9. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, in a command prompt, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

Next, you must run the Oracle Data Guard configuration on the standby server (refer to page 101).

Running the Oracle Data Guard configuration on the standby server

(Topic number: 123967)

After the Data Guard configuration is run on the primary server and before running the configuration on the standby server, the listener needs to be started.

To start the public listener

1. Log in as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Type **lsnrctl start listener_public**.

After the listener service is started, run the Oracle Data Guard configuration on the standby server.

To run the Oracle Data Guard configuration on the standby server

1. On the standby server, log in as user **root** (Solaris) or **AgfaService** (Windows).
2. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
3. On Solaris, type **./setup_dg**.

   or

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt by selecting **Start**, then right-clicking **Command Prompt**, then selecting **Run as administrator**. Then, type **bash setup_dg**
4. When prompted, provide the Flashback area and host name information requested.
5. When asked if you want to do the RMAN restore, type **"n"**.
6. When asked about the manual restore, start up a separate prompt on the standby server and perform the procedures that follow to restore the database on the standby server in the new command prompt.

   For the time being, leave the existing prompt alone.

Next, if using Solaris servers, share the primary Flashback Recovery Area and primary /dbase partition; otherwise, if using Windows servers, restore the database on the standby server (refer to page 102).

Restoring the database on the standby server

(Topic number: 124004)

Restoring the database on the standby server is required for both Solaris and Windows servers.

To restore the database on the standby server

1. Log into the primary server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. Shut down the primary server by typing

   sqlplus / as sysdba

   shutdown immediate;

   exit;
3. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
4. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory
5. On Solaris, type

   mv orapw orapw.pre_dg

orapwd file=orapw password=stayout entries=40

On Windows, type

mv PWDMVF.ora PWDMVF.ora.pre_dg

orapwd file=PWDMVF.ora password=stayout entries=40

This creates an Oracle password file.

6. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

7. To shut down the standby database, type

   sqlplus / as sysdba

   shutdown immediate;

   exit;

8. On Solaris, to mount the partition locally, log in as the **root** user and type

   mount *primary_server_name*:*path_to_flashback_recovery_area_on_primary_server* /mnt1

   mount *primary_server_name*:/dbase /mnt2

9. Clean up the existing data files and redo log files from the standby server by deleting (or move) these files. In doing so, ensure that the /dbase directory structure and any symlinks remain untouched.

/dbase/system/*.ctl	/dbase/redo/*.dbf	/dbase/data1/*.ctl
/dbase/system/*.dbf	/dbase/index1/*.ctl	/dbase/data1/*.dbf
/dbase/rbs/*.ctl	/dbase/index1/*.dbf	/dbase/data2/*.ctl
/dbase/rbs/*.dbf	/dbase/index2/*.ctl	/dbase/data2/*.dbf
/dbase/redo/*.ctl	/dbase/index2/*.dbf	/dbase/arch/*.dbf

10. Copy the necessary data files and redo log files from the primary server to the standby server:

Note:

On Solaris, use the **cp -rp** command for each. On Windows, use standard file copy and paste functionality.

Source directory	Source files	Target directory	Additionally
flashback/ db_recovery_area	standby_control.ctl	flashback/*db_recovery_area*	–

Source directory	Source files	Target directory	Additionally
/mnt2/data1	All files with *.dbf extensions	/dbase/data1 (Solaris) or D:\data\dbase\data1 (Windows)	If you have data2/data3/data4 directories that are not symlinks of data1, also copy to those directories.
/mnt2/index1	All files with *.dbf extensions	/dbase/index1 (Solaris) or D:\data\dbase\index1 (Windows)	If you have index2/index3/index4 directories that are not symlinks of index1, also copy to those directories.
/mnt2/system	All files with *.dbf extensions	/dbase/system (Solaris) or D:\data\dbase\system (Windows)	If you have rbs/redo directories that are not symlinks of system, also copy to those directories.
/mnt2/system	All redo0*.log files	/dbase/system (Solaris) or D:\data\dbase\system (Windows)	Make sure the redo_standby*.log files are not copied. Note that the redo log files could be in the redo directory.

11. Copy any additional data or index files from the primary to the standby server, but do **not** copy the control files or the standby redo log files.
12. On the standby server, restore the standby control file in RMAN.
    a. Log in as user **oracle** (Solaris) or **AgfaService** (Windows).
    b. Type

       rman target /

       startup nomount;

       restore standby controlfile from *'flashback/db_recovery_area directory*/standby_control_file.ctl';

       shutdown abort;

       startup mount;

       exit
13. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
14. On the standby server, switch back to the command prompt where setup_dg was running. At the manual restore prompt, type **"y"** to continue with Data Guard configuration.

Finally, to link the two servers, complete the Data Guard configuration (refer to page 105).

Completing the Data Guard configuration

(Topic number: 124015)

Linking the two servers, a final Oracle Data Guard configuration task is necessary.

To complete the Data Guard configuration

1. Log into the primary server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
2. If the primary database is not started, start it up by typing

   sqlplus / as sysdba

   startup;

   exit;
3. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
4. To continue the Oracle Data Guard configuration, log in as **root** (Solaris) or **AgfaService** user (Windows).
5. On Solaris, type **./setup_dg**.

   On Windows Server 2008, either 32-bit or 64-bit, open an elevated command prompt. To open an elevated command prompt, select **Start**, right-click **Command Prompt**, then select **Run as administrator**.

   On Windows, type **bash setup_dg**.
6. At the prompt, `About to enable log_archive_dest_1 on Primary. Has Data Guard been configured on the Standby?`, type **"y"**.
7. When prompted, manually copy the **tnsnames.ora.client** file to the Oracle Client stations.
8. On Solaris systems, manually copy the **/export/mvf/odbc32v52/odbc.ini** file to the same location on the Network Gateway servers.

Next you must configure RMAN backups (refer to page 105) on the primary and standby servers.

Configuring RMAN backups after the Oracle Data Guard configuration

(Topic number: 66586)

Perform this task after you have backed up the database on the primary server and restored it on the standby server as part of the Oracle Guard configuration.

Configuring RMAN to perform a disk backup at this point cleans up the archive logs.

To configure RMAN backups after the Oracle Data Guard configuration

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.

2. In a command prompt, change to the **/usr/mvf/bin** (Solaris) or the **C:\mvf\bin** (Windows) directory.
3. Run the **configure_backup** command.
4. To create a standby control file on the primary server, type

   sqlplus / as sysdba

   alter database create standby controlfile as '/opt/oracle/standby_control_file.ctl';
5. Copy the control file, **standby_control_file.ctl**, from the primary to the standby server.

   On Solaris, you can use the following command to do so:

   scp /opt/oracle/standby_control_file.ctl service@*host_name_of_standby_server*/usr/mvf

   On Windows, use standard copy and paste functionality to copy the file over.
6. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.
7. Run the **configure_backup** command on this server as well.
8. To shut down the standby server, type the following:

   sqlplus / as sysdba

   shutdown immediate;
9. To import the standby control files from the primary server to the standby server, first rename them with a **.orig** extension on the standby server; for example, change **control03.ctl** to **control03.ctl.orig**. The files to rename are:
   a. **/usr/mvf/data/dbase/data2/control03.ctl** (Solaris) or **E:\data\dbase\data2\control03.ctl** (Windows)
   b. **/usr/mvf/data/dbase/index2/control02.ctl** (Solaris) or **E:\data\dbase\index2\control02.ctl** (Windows)
   c. **/usr/mvf/data/dbase/system/control01.ctl** (Solaris) or **E:\data\dbase\system\control01.ctl** (Windows)
10. Now copy the standby control files from the primary server to the standby server. The files to copy are the same as those listed in the previous step.
11. To start and mount the standby server, type

    sqlplus / as sysdba

    startup mount

Maintaining Oracle Data Guard

(Topic number: 67248)

Data Guard is Oracle's high-availability solution, using primary and standby database servers. Once this solution is configured, ongoing maintenance is required to ensure system availability.

Synchronizing redo changes from the primary database to the standby database

(Topic number: 67142)

Changing the size and number of the online redo log files is sometimes done to tune the database. You can add or drop online redo log file groups or members to the primary database without affecting the standby database. Similarly, you can drop log file groups or members from the primary database without affecting the standby database. However, these changes can affect the performance of the standby database after switchover.

For example, the primary database has 10 redo log files and the standby database has two online redo log files. When you switch over to the standby database so that it functions as the new primary database, the new primary database is forced to archive more frequently than the original primary database.

We strongly recommend that if you add or drop online redo log files from the primary database, you synchronize the changes on the standby database.

To synchronize redo changes from the primary database to the standby database

1. If Redo Apply is running, you must cancel it before you can change the log files. In sqlplus on the standby server, execute the command:

   alter database recover managed standby database cancel;

2. If the STANDBY_FILE_MANAGEMENT initialization parameter is set to AUTO, to change the value to MANUAL, execute the command:

   alter system set standby_file_management = manual;

3. To add or drop an online redo log file, execute the commands:

   connect internal

4. To check the existing redo log groups, execute the command

   select * from v$log;

5. To determine the location and the file names of the current redo log files, execute the command

   select * from v$logfile;

6. To add a new online redo log file, execute the command

   alter database add logfile 'usr/mvf/data/dbase/redo/redo#.log' size 25000K; (Solaris) or **alter database add logfile 'd:\data\dbase\redo\redo#.log' size 25000K;** (Windows)

   Where # is the number of the next redo log group. For example, if the **select * from v$logfile;** command returns redo03, you would create redo04.

7. To add more redo log files, repeat steps 5 and 6.

8. To switch to the current log file, execute the command:

   alter system switch logfile;

9. If the redo log needs to be dropped, execute the commands:

   alter database drop logfile group #;

select * from v$log;

Where # specifies the log group to drop, for example, **alter database drop logfile group 1;** drops the redo01.log file

10. To restore the STANDBY_FILE_MANAGEMENT initialization parameter and the Redo Apply options to their original states, execute the commands:

    alter database recover managed standby database using current logfile disconnect from session;

    alter system set standby_file_management = auto;

Rebooting the standby database server

(Topic number: 67099)

If you have to do any type of servicing of the standby server, you can reboot the server after the servicing.

To reboot the standby database server

1. Log into the standby server.

   On Solaris, log in as the **root** user. On Windows, log in as the **AgfaService** user.
2. To prevent IMPAX from starting after a reboot, in a command prompt, type

   # disable_impax
3. If running on Windows, ensure all the IMPAX services are set to **Manual** startup.
4. Change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
5. To reboot the standby server, type

   $ sqlplus / as sysbda

   alter database recover managed standby database cancel;

   shutdown immediate;
6. Change to the root directory.
7. Reboot the Windows server or on Solaris, type **# init 6**.
8. After the standby server reboots, change to the **/usr/mvf/bin** (Solaris) or **C:\mvf\bin** (Windows) directory.
9. To start the Oracle Managed Recovery Process, type

   $ sqlplus / as sysbda

   startup mount;

   alter database recover managed standby database using current logfile disconnect from session;

   exit;
10. To start the private listener, type

lsnrctl start listener

Rebooting the primary database server

(Topic number: 67102)

If you have to do any type of servicing of the primary server, you can reboot the server after the servicing.

To reboot the primary database server

1. Reboot the primary server.

   On Solaris, log in as the **root** user and type **init 6**. On Windows, reboot the server.

2. After the reboot, verify that the public listener is started.

   On Solaris type **psg tns**. On Windows check that the **OracleohomeTNSListener_listener_public** service is started.

3. Start the public listener if not already started.

   On Solaris type**lsnrctl start listener_public**. On Windows, start the **OracleohomeTNSListener_listener_public** service.

Resizing Oracle data files

(Topic number: 67133)

You must run the **monitor_add** or **monitor_resize** command to increase or resize the Oracle data files before propagating the file changes to the standby database.

To resize Oracle data files

1. Log into the primary server, log into sqlplus as the **sys** user.
2. Execute the command

   alter system switch log file;

Removing the Oracle Data Guard configuration on the primary and standby servers

(Topic number: 67105)

If you want to uninstall Oracle Data Guard or completely reconfigure it, you can remove the Oracle Data Guard configuration on the primary and standby servers.

To remove the Oracle Data Guard configuration on the primary and standby servers

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.

2. In a command prompt, to run Data Guard manager, type

dgmgrl sys/stayout@MVF1

3. In Data Guard manager, to remove the Data Guard configuration, type

   remove configuration

4. Remove the Data Guard configuration files from the primary server.

   On Solaris, type

   cd /opt/oracle/current/dbs

   rm dr*.dat

   On Windows, delete the **dr*.dat** file from C:\oracle\product\10.2.0\db_1\database.

5. Save all the edited Data Guard files such as initMVF.ora, spfileMVF.ora, tnsnames.ora, and listener.ora. To make a copy of these files, type

   On Solaris:

   cd /opt/oracle/current/dbs

   cp initMVF.ora initMVF.ora.dg_save

   cp spfileMVF.ora spfileMVF.ora.dg_save

   cd /var/opt/oracle

   cp tnsnames.ora tnsnames.ora.dg_save

   cp listener.ora listener.ora.dg_save

   On Windows:

   cd C:\oracle\product\10.2.0\db_1\database

   cp initMVF.ora initMVF.ora.dg_save

   cp spfileMVF.ora spfileMVF.ora.dg_save

   cd C:\oracle\product\10.2.0\db_1\network\ADMIN

   cp tnsnames.ora tnsnames.ora.dg_save

   cp listener.ora listener.ora.dg_save

6. To turn off flashback, type

   sqlplus / as sysdba

   alter database flashback off;

7. To turn off force logging, type

   alter database no force logging;

8. Halt all the job queues.
9. Stop IMPAX and IIS on the core servers.
10. To shut down the database, type

    sqlplus / as sysdba

    shutdown immediate;

11. Revert the edited files (listener.ora, tnsnames.ora, spfile.ora) to the original files. To copy the original initMVF.ora, tnsnames.ora and listener.ora files back to their respective locations, type

    On Solaris:

    cd /opt/oracle/current/dbs

    cp –rp initMVF.ora.pre_dg initMVF.ora

    cd /var/opt/oracle

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

    On Windows:

    cd C:\oracle\product\10.2.0\db_1\database

    cp –rp initMVF.ora.pre_dg initMVF.ora

    cd C:\oracle\product\10.2.0\db_1\network\ADMIN

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

12. To create the spfile from the pfile, type

    sqlplus / as sysdba

    create spfile from pfile;

13. To start the database, type

    startup;

14. Modify crontab (Solaris) or Task Scheduler (Windows) and remove references to Oracle Data Guard.

    On Solaris:

    Comment the **15 20 * * * /usr/mvf/bin/check_if_primary_db && /usr/mvf/bin/check_standby** crontab entry out by adding a **#** at the beginning of the line.

    On Windows:

    Disable or delete the **CheckStandby** task in Task Scheduler.

15. Repeat the previous steps on the standby server.
16. On the core servers, restart IMPAX and IIS.
17. Restart all the job queues.
18. To ensure that IMPAX starts successfully, test the primary database server.
19. Test the IMPAX Client connectivity.

Switching over to the standby server

(Topic number: 67114)

If you want to service the primary server, you can switchover to the standby server.

The public listener on the current standby server has not been set. To avoid IMPAX Client connectivity problems, you must stop listener_public on the primary server when the primary database goes down. You can then switchover to the standby server, run the standby database, and reinstate the former primary server. During this time, the IMPAX Client can still connect to the database, which is running on the standby Oracle Data Guard host.

To switch over to the standby server

1. Stop the public listener on the primary server.

   On Solaris, as the oracle user, type **lsnrctl stop listener_public**. On Windows stop the **public_listener** service.

2. To stop IMPAX on the primary server, as the root user, type

   stop_impax (Solaris) or **stopall** (Windows)

3. To launch the Data Guard manager on the primary server and perform the switchover, as the Oracle user, type

   dgmgrl sys/stayout@mvf1

   show configuration

   switchover to 'MVF2'

   show configuration

   exit

4. Start the public listener on the standby server, which has been promoted to the primary server.

   On Solaris, as the oracle user, type **lsnrctl start listener_public**.

   On Windows, start the **public_listener** service.

5. To query for the ae_ref and the ae_title, in CLUI, type

   ae query

6. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref = map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='*AE_title_of_failed_primary_server*'

   Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete *service_ref*

8. To set the new primary Task Scheduler, in CLUI, type

   update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

   update mvf_ts_config set ae_ref='*AE_title_of_new_primary_server*' where ae_ref='*AE_title_of_failed_server*'

9. To start IMPAX on the new primary server, as the root user, type

start_impax (Solaris) or **startall** (Windows)

10. As the root user, restart the MVF Task Scheduler on the remaining IMPAX servers such as the Archives, Network Gateways, and Curators.

    On Solaris, restart the MVF Task Scheduler by killing the process or restarting IMPAX. On Windows, restart the Mitra System Task Scheduler service.

Note:

If this is the first time that the standby database is opened after a switchover, re-create the temporary file on the standby server (refer to page 114).

The IMPAX Clients can now connect to the new primary database. After the switchover, the Client may continue to experience connectivity problems, specifically in the Image area, but should be resolved on its own a few minutes after switchover as IMPAX re-establishes the connection to the newly promoted database server.

Failing over to the standby server

(Topic number: 67117)

If the primary server is unavailable, you can fail over to the standby server to ensure maximum availability.

To fail over to the standby server

1. If you can connect to the primary server, stop the public listener.

   On Solaris, as the oracle user, type**lsnrctl stop listener_public**.

   On Windows, stop the **public_listener** service.

   If you cannot connect to the primary server, skip to step 3.

2. To stop IMPAX, as the root user on the primary server, type

   stop_impax (Solaris) or **stopall** (Windows)

3. To launch the Data Guard manager on the standby server and perform the failover, as the oracle user on Solaris or the AgfaService user on Windows, type

   dgmgrl sys/stayout@mvf2

   show configuration

   failover to 'MVF2'

   show configuration

   MVF2 is now the primary server.

4. Start the public listener on the standby server, which has been promoted to the primary server.

   On Solaris, as the oracle user, type **lsnrctl start listener_public**. On Windows, start the public_listener service.

5. To query for the ae_ref and the ae_title, in CLUI, type

ae query

6. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref = map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='<AE Title of the failed primary server>'

   Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete <*service ref*>

8. To set the new primary Task Scheduler, in CLUI, type

   update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

   update mvf_ts_config set ae_ref='*AE_title_of_new_primary_server*' where ae_ref='*AE_title_of_failed_server*'

9. To start IMPAX on the new primary server, as the root user, type

   start_impax (Solaris) or **startall** (Windows)

10. As the root user, restart the MVF Task Scheduler on the remaining IMPAX servers such as the Archives, Network Gateways, and Curators.

    On Solaris, restart the MVF Task Scheduler by killing the process or restarting IMPAX. On Windows, restart the Mitra System Task Scheduler service.

Note:

If this is the first time that the standby database is opened after a failover, you must re-create the temporary file on the standby server (refer to page 114).

The IMPAX Clients can now connect to the new primary database. After the switchover, the Client may continue to experience connectivity problems, specifically in the Image area, but should be resolved on its own a few minutes after switchover as IMPAX re-establishes the connection to the newly promoted database server.

Re-creating the temporary file on the standby server

(Topic number: 67286)

If this is the first time that the standby database is opened after a switchover or failover, you must re-create the temporary file on the standby server.

To re-create the temporary file on the standby server on Windows

1. To log into sqlplus, from the command line, type

   sqlplus sys/stayout as sysdba

2. To add a new temp file to F:\DATA\DBASE\SYSTEM, type

   alter tablespace TEMP add tempfile 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' SIZE 500M REUSE;

3. To bring the original temp file offline and bring the new one online, type

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' OFFLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' ONLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' DROP;

4. To recreate TEMP01.DBF, type

   alter tablespace TEMP add tempfile 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' SIZE 500M REUSE;

5. To bring TEMP01.DBF online and to drop TEMP02.DBF, type

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' OFFLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP01.DBF' ONLINE;

   alter database TEMPFILE 'F:\DATA\DBASE\SYSTEM\TEMP02.DBF' DROP;

To re-create the temporary file on the standby server on Solaris

1. To log into sqlplus, from the command line, type

   sqlplus sys/stayout as sysdba

2. To add a new temp file to F:\DATA\DBASE\SYSTEM, type

   alter tablespace TEMP add tempfile '/usr/mvf/data/dbase/system/temp02.dbf' SIZE 500M REUSE;

3. To bring the original temp file offline and bring the new one online, type

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' OFFLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' ONLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' DROP;

4. To recreate TEMP01.DBF, type

   alter tablespace TEMP add tempfile '/usr/mvf/data/dbase/system/temp01.dbf' SIZE 500M REUSE;

5. To bring TEMP01.DBF online and to drop TEMP02.DBF, type

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' OFFLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp01.dbf' ONLINE;

   alter database TEMPFILE '/usr/mvf/data/dbase/system/temp02.dbf' DROP;

Reinstating the failed primary database

(Topic number: 67120)

Once the failed primary server has been repaired, you can reinstate it as the primary database.

To reinstate the failed primary database

1. After the primary database has been repaired, to restart the database, as the oracle user on Solaris or the AgfaService user on Windows, type

   sqlplus / as sysdba

   startup mount;

   quit

2. To launch the Data Guard manager, on the primary server as the oracle user on Solaris or the AgfaService user on Windows, type

   dgmgrl sys/stayout@mvf2

3. To perform the switchover type

   show configuration

   reinstate database 'MVF1'

   show configuration

   exit

4. To launch the Data Guard manager on the repaired primary, as the Oracle user, type

   dgmgrl sys/stayout@mvf2

5. To make MVF1 the primary server type

   switchover to 'MVF1'

   exit

6. Stop the public listener on the new standby server.

   On Solaris, as the oracle user, type**lsnrctl stop listener_public**. On Windows, stop the **public_listener** service.

7. To stop IMPAX on the new standby server, type

   stop_impax (Solaris) or **stopall** (Windows)

8. To query for the ae_ref and the ae_title, in CLUI, type

   ae query

9. To determine the signal translator service refs, in CLUI, type

   select map_service.service_ref from map_service inner join map_ae on map_ae.ae_ref = map_service.ae_ref inner join map_implements on map_service.service_ref = map_implements.service_ref inner join map_process on map_implements.process_ref = map_process.process_ref where map_process.process_title='MVF_SIGNAL_TRANSLATOR' and map_ae.ae_title='*AE_Title_of_ failed_primary_server*'

Two service refs are returned.

10. For each service ref, in CLUI, type

    service delete <*service ref*>

11. To set the new primary Task Scheduler, in CLUI, type

    update map_ini set ini_value='*AE_title_of_new_primary_server*' where ini_section='MVF_TASK_SCHEDULER' and ini_key='PRIMARY_SERVER'

    update mvf_ts_config set ae_ref='*AE_reference_of_new_primary_server*' where ae_ref='*AE_reference_of_old_primary_server*'

12. Start the public listener on the new primary server.

    On Solaris, as the oracle user, type **lsnrctl start listener_public**. On Windows, start the **public_listener** service.

13. To start IMPAX on the new primary server, as the root user, type

    start_impax (Solaris) or **startall** (Windows)

Tools for monitoring Oracle Data Guard

(Topic number: 66589)

Oracle Data Guard is a high-availability solution that uses two database servers—the active, primary server, and a standby server that can take over should any problems occur on the primary server. The following tools are available for monitoring an Oracle Data Guard configuration.

Script	Description
check_dg_configuration	Used to sanity check an existing Data Guard configuration to see if the init parameters are set as expected. Run this script manually, as necessary. It works only on the primary server. **Note:** On Windows 2008, run check_dg_configuration from an elevated command prompt.
check_standby	Configured through crontab (AS3000) or Scheduled Tasks (AS300) to run daily at 3:45 and 20:15 to detect any archive gaps between the primary and standby servers. If the gap exceeds 20, an exception is sent. This script works only on the primary server.

Tip:

To run these scripts on Windows, precede them with **bash**; for example **bash check_dg_configuration**.

Troubleshooting: The application encountered a problem with the standby database

(Topic number: 66656)

Issue

The following error message appears in the Exception Viewer:

```
The application encountered a problem with the Standby database
```

Details

This message applies only when using an Oracle Data Guard configuration, with a primary and standby database. It indicates that the archive gap between the primary and standby databases exceeds 20.

Solution

Perform diagnostics such as the following.

1. To verify that the listener.ora files on both the primary and standby servers are correct, log into the primary server as the oracle user on Solaris and the AgfaService user on Windows.

   Change to the **/usr/mvf** (Solaris) or **C:\mvf\bin** (Windows) directory and type the following

   tnsping MVF

   tnsping MVF1

   tnsping MVF2
2. Ensure that the standby server is up and running.
3. Ensure that the private listener is running on the standby by typing:

   lsnrctl status
4. Look for errors in the following logs, on both the primary and standby servers:

   /usr/mvf/data/logs/oracle/bdump/alert_MVF.log and arcMVF.log (Solaris)

   C:\mvf\data\logs\oracle\bdump (Windows)
5. Ensure that Oracle is running on the standby server by typing **psg ora**.
6. To confirm that the redo log has been set on both the primary and standby server, execute the following command in sqlplus on the primary server, then repeat it on the standby server. Ensure that the list matches between the two servers.

   select * from v$logfile
7. Ensure that the last line of the redo log contains the standby log files; for example, /usr/mvf/data/dbase/redo/redo_stdby07.log (Solaris) or d:\data\dbase\redo\redo_stdby07.log (Windows).
8. To check that the log files are being received and applied on the standby server, in sqlplus, execute the command

select sequence#,applied from v$archived_log order by sequence#;

9. To force a log switch on the primary server, execute the command

   alter system switch logfile;

10. Check again to ensure that the log files are being received and applied on the standby server. Execute the command

    select sequence#,applied from v$archived_log order by sequence#;

    Ensure that one additional entry appears in the list.

11. To check the configuration, on the primary server, open the Data Guard manager:

    dgmgrl sys/stayout@mvf1

    show configuration;

Installing an IMPAX AS300 single-server

C

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:

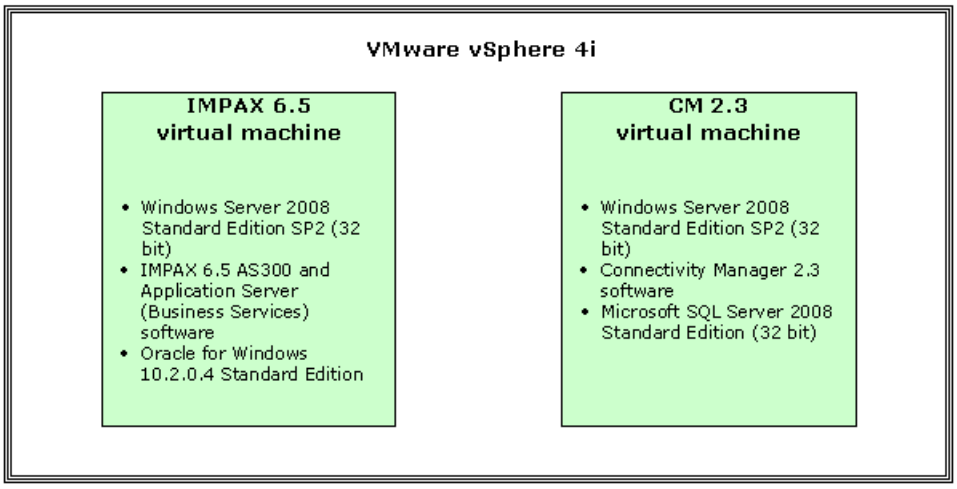
To upgrade an AS300 single-server from IMPAX 6.3 or earlier, a re-install of IMPAX and Connectivity Manager is necessary. To upgrade from IMPAX 6.4 or later, or for assistance in upgrading from IMPAX 6.3 or earlier, contact Agfa Professional Services.

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 *Installing an IMPAX AS300 single-host server* (refer to page 42).

5. Install and configure the Application Server.

   Refer to the *IMPAX 6.5.1 Application Server Installation, Upgrade, and Configuration Guide* for detailed installation and configuration instructions.

AS3000 portable password file

D

If installing an AS3000 Database Server, you need to generate the portable password file on the AS3000 database.

Generating and importing mvf.portable.psd

(Topic number: 6980)

System security is enforced by having credentials for IMPAX internal processes contained within encrypted password files that must be distributed to all machines in the cluster.

When installing IMPAX on the Database Server, the impax_install script uses a passkey utility to save the AgfaService password to a password file at /usr/mvf/mvf.psd. Next the utility creates a portable version of this password file at /usr/mvf/mvf.portable.psd.

When installing IMPAX Network Gateway or Archive Server software, the IMPAX installation script imports mvf.portable.psd, re-encrypts it using a machine specific key, and creates the file /usr/mvf/mvf.psd on the target server.

In some cases the mvf.portable.psd file is not available on the Database Server. This does not prevent any of the initial Network Gateway or Archive Server installs, but you must manually generate and import the password key to the target server.

In other cases following initial installations, prudent security management recommends that the mvf.portable.psd file be deleted from the Database Server once all Network Gateway and Archive Server machines are installed. Therefore, if at some later point you install a new Network Gateway or Archive Server, you must manually generate and import the password key to the target server.

Whenever the import of mvf.portable.psd to the target server fails during an AS3000 installation, you see the following log message indicating the required password file is not on the Database Server:

```
The AgfaService ID password file failed to import properly. You will need to
import the password file manually.
```

The AS3000 Network Gateway or Archive Server installation completed successfully (unless other log messages indicate otherwise), but you must manually generate and import the password key to the target server.

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 locally to the target server

(Topic number: 58086)

Once generated, you can import the password file onto the server that needs it.

To import the portable password file locally to the target server

1. Log into the target Network Gateway or Archive Server as the **root** user.
2. To import the portable password file, type

   /usr/mvf/bin/passkey -M IMPORT -k *temporary_password*

   where *temporary_password* is the password you gave when exporting the portable password file.

   This reads the mvf.portable.psd file, re-encrypts it using a machine specific key, and creates the local /usr/mvf/mvf.psd file.
3. To restrict permissions on the newly created mvf.psd file, type

   chmod 640 /usr/mvf/mvf.psd
4. Delete /usr/mvf/mvf.portable.psd from the target server.

CAUTION!

The mvf.portable.psd file contains sensitive information. To maintain the security of the system, the portable password file should be deleted both the Database Server and the target servers.

Troubleshooting IMPAX

E

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

Troubleshooting: Installation of IMPAX software unsuccessful; must reinstall packages

(Topic number: 7685)

Issue

IMPAX Server was not installed successfully.

Details

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

Solution

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

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

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

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

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

To uninstall the IMPAX software

1. Open Control Panel.
2. In Windows 2003, select **Add or Remove Programs**.

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

   Important!

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

You can then reinstall the IMPAX packages.

Troubleshooting: Reinstalling Oracle on Windows

(Topic number: 121676)

Issue

In rare circumstances, if you are experiencing one or more problems with Oracle on Windows that cannot be resolved by the usual troubleshooting techniques, you may have to reinstall Oracle on Windows.

CAUTION!

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

Solution

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

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

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

   CAUTION!

   Serious problems might occur if you modify the registry incorrectly. These problems might require that you reinstall your operating system and there is no guarantee that these problems can be solved. We recommend that you back up the registry before you change it, so that you can back out the changes if necessary.
6. Select **Start** > **Oracle - ohome** > **Oracle Installation Products** > **Universal Installer**.
7. Select **Deinstall Products**.
8. Under Oracle Homes, select the **ohome** checkbox, then click **Remove**.
9. Click **Yes** to start the deinstallation.
10. When the deinstallation is done, restart the server, then log into Windows as an administrator-level user.
11. If the C:\oracle directory still exists, delete it.
12. If the C:\Program Files\oracle directory still exists, delete it.
13. Delete the registry key HKEY_LOCAL_MACHINE\Software\ORACLE.
14. If any files or directories reside in C:\cygwin\tmp, delete them.
15. Create a directory on the C:\ drive to store files that you will back up in the next step.

16. Move the C:\oracle_drives, C:\Oracle_install.log, and C:\installOracleInfo files into the directory you created in the previous step.
17. Restart the server, then log into Windows as an administrator-level user.
18. Use the OracleInstall package to install Oracle Server (refer to page 35).
19. After the installation finishes, copy the backup files you created in steps 3 and 5 into the original directories.
20. Re-create the MVF and MVF_ORA ODBC System Data Source Names (DSNs) as needed.

Note:

The AS300 installation automatically creates the MVF DSN.

Troubleshooting: Server license keys do not work

(Topic number: 7649)

Issue

Programs do not start because of Server license key problems.

Details

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

Solution

Ensure that the appropriate license keys are installed in the correct location. Information on obtaining a MAC address is available in *Obtaining Server license keys* (refer to page 40).

CAUTION!

Because you may be installing the mvf and archive licenses on the same station, to prevent the mvf license key from being overwritten, ensure that you rename the mvf license key before copying the archive license key into the mvf directory.

To install the mvf license key

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

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

To install the archive license key

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

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

Troubleshooting: Cannot connect to the Administration Tools

(Topic number: 7740)

Issue

You cannot log into the Administration Tools.

Details

Two possibilities exist for this problem:

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

Solutions

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

To stop and restart the Administration Tools service

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

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

To modify the default port range

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

   netstat -a
3. Ports within the 1200-1270 range with a state of LISTENING do not have to be modified. If you find that the ports within that range do not have a state of LISTENING:

a. In a text editor, open **C:\mvf\java\etc\jserver.properties**.
b. Search for **jmtk.rmiPortRange=1200-1270**.
c. Modify the range to suit the needs of the site.
d. Save and close the modified file.

Troubleshooting: 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: Uninstalling IMPAX 6.5.1 Server

(Topic number: 121736)

Issue

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

Solution

1. Open Control Panel.
2. Depending on the version of Windows, select **Add or Remove Programs** or **Programs and Features**.
3. Under Currently installed programs, select **AGFA IMPAX AS300**.
4. Click **Change**.
5. At the prompt, type your name and click **Next**.
6. At the Welcome dialog, select **Modify**. Click **Next**.
7. Clear the checkboxes of any AS300 packages to uninstall. Select the checkboxes of any packages to install.
8. Click **Next**.
9. In the Maintenance Complete dialog, select **Yes, I want to restart my computer now** and click **Finish**.
10. If no longer required on this server, you can also delete any Server license files stored in the C:\mvf directory.

    Licenses are required if the MVFNetworkGateway package is installed, or if the server is being used for archiving (HSM or PACS Store and Remember).

Integrating the IMPAX Enterprise Solution

F

The IMPAX Enterprise Solution offers a fully integrated RIS, PACS, and Reporting solution.

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.

Security, archive, and license references

G

If you are using an Oracle Database Server on a Solaris host (in a mixed-host configuration), also refer to the Appendixes of the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

Types of archives

(Topic number: 7209)

Tip:

For more details on archive functionality, refer to the Archive Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

Supported archive configurations:

- HSM (Hierarchical Storage Management)
- PACS Store and Remember

HSM archives

(Topic number: 11577)

The HSM archive system provides long-term storage of data and access to data. Studies archived with HSM are stored to a file system. A mount point and subdirectory to store studies to is specified. The HSM system takes care of storing the data.

Before storing or retrieving data, ensure that the mounted location is set up properly and is ready for storage and retrieval of files.

PACS Store and Remember

(Topic number: 6941)

A PACS Store and Remember archive is an IMPAX Server computer that acts as an Archive Server, where the images are stored on a PACS archive external to the IMPAX system. Any IMPAX Server computer with a cache that is not currently an Archive Server can be set up as a Store and Remember archive. The PACS Store and Remember archive is aware of the studies that exist on the external archive, but is not aware of precisely where on the external archive these studies are stored. The external archive takes full responsibility for permanently archiving studies.

PACS Store and Remember archiving works the same way as other archiving. You configure the archiving based on the station, Autopilot creates STORE jobs based on the archiving settings, and studies can be retrieved via RETRIEVE jobs. A PACS Store and Remember queue is a DRIVE queue that is managed like any other DRIVE queue in the Administration Tools.

The difference between PACS Store and Remember archiving and media-based archiving is that the mvf-scu process handles the archiving, instead of a separate archive process. Also, a STORE job is done via DICOM C-STORE, and a RETRIEVE job is done via DICOM C-MOVE.

Securing Windows-based systems in IMPAX (armoring): Reference

(Topic number: 9311)

Changes are made during the Application Server installation and armoring procedure to ensure that the Application Server system is as secure as possible without affecting the functionality of the system. The following security measures are enforced during the armoring procedure:

- All unnecessary services and applications are disabled (refer to page 138).
- Insecure network services are disabled.
- The ODBC tracing executable is disabled. Disabling this executable ensures that user names and passwords are always encrypted in the trace log.
- Optional services and applications are not installed.
- All IMPAX services are configured to run under restricted user accounts that can access only the resources they need. These accounts are created during the IMPAX installation.
- A default list of firewall rules is added to the system automatically, blocking external access to unused ports where unsecured services could reside if accidentally configured and started. The default rules are sufficient in most cases, but new rules can be added to increase security for a particular setup.

Groups and accounts created for IMPAX

During the IMPAX installation, the ImpaxServerGroup is created and the list of files that this group has full access to is configured. The Administrators group is automatically created by Windows, however, the list of files that this group has access to (refer to page 139) is modified during the IMPAX installation.

The following accounts are created by the IMPAX installation program.

Account	Groups that it belongs to	Services that run under the account
ImpaxServerUser	• ImpaxServerGroup	• AgfaHealthcare • IMPAX App Server Data Manager • IMPAX Audit Event Log Manager • IMPAX Distributed License Manager • IMPAX Messaging Service
AgfaService	• Administrators	• Administrator account used by Agfa support

Note:

For a service on one machine in a network to access the resources (files and folders) that it needs on another machine in the network, a user account with the same user ID and password must be created on each machine. The user IDs and passwords are maintained in an encrypted password file on the Database Server, as explained in *Generating the AS300 portable password file* (refer to page 57).

List of services disabled by the IMPAX installation: Reference

(Topic number: 9309)

The following services are disabled by the IMPAX installation. The Background Intelligent Transfer and Print Spooler services may be manually enabled on some systems to provide access to print functions and for the PACS Client Updater.

Note:

Any services that explicitly depend on these services will fail to start.

Name of service	Description of service
Background Intelligent Transfer	Used to download files from an HTTP server using idle network bandwidth allowing no interfering with client browsing.

Name of service	Description of service
Computer Browser	Allows a computer to act as a browser master to keep a list of computers that exists on a network.
Distributed File System	Integrates disparate file shares into a single, logical namespace and manages these logical volumes distributed across a local or wide area network.
Distributed Link Tracking Client	Enables client programs to track linked files that are moved within an NTFS volume, to another NTFS volume on the same computer, or to an NTFS volume on another computer.
Distributed Transaction Coordinator	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems.
Print Spooler	Manages all local and network print queues and controls all printing jobs.
Windows Audio	Manages audio devices for Windows-based programs.
Windows Error Reporting Service (Windows Server 2008)	Collects, stores, and reports unexpected application crashes to Microsoft.
Windows Update (Windows Server 2008)	Enables the download and installation of Windows updates for Windows Server 2008.
WinHTTP Web Proxy Auto-Discovery Service	Implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol to enable an HTTP client to automatically discover a proxy configuration.
Wireless Configuration	Enables automatic configuration for IEEE 802.11 adapters.

The following services are set to manual by the IMPAX installation.

Name of service	Description
Cryptographic Services	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Key Service, which helps enroll this computer for certificates.

Files that IMPAX groups have access to: Reference

(Topic number: 9308)

The ImpaxServerGroup is created during the IMPAX installation. That group and the IIS_WPG group have full access rights to the following folders:

ImpaxServerGroup

Access type	Locations
Full	C:\Program Files\Agfa\Impax Business Services\Messaging Service

Access type	Locations
	C:\Program Files\Agfa\Sec\audit\log
	C:\Program Files\Agfa\Impax Business Services\License Manager
	C:\Program Files\Agfa\Impax Business Services\Audit Event Log Manager

IIS_WPG

Access type	Locations
Read/Execute	C:\Impax\CDExport
	E:\inetpub\wwwroot\AgfaHC.Connectivity.Web.Services
	E:\inetpub\wwwroot\AgfaHC.Messaging.Server.WebServices
	E:\inetpub\wwwroot\AgfaHC.Pacs.Web
	E:\inetpub\wwwroot\AgfaHC.Pacs.Web.Services
	E:\inetpub\wwwroot\AgfaHC.RIS.Web.Services
	E:\inetpub\wwwroot\AgfaHC.User.Web.Services
	E:\inetpub\wwwroot\AgfaHC.User.Security.Web.Services
	E:\inetpub\wwwroot\AgfaHC.User.Administration.Web.Services
	C:\Oracle
Full	C:\Impax\Logs
	C:\Program Files\Agfa\Sec\audit\log

Understanding the passkey utility

(Topic number: 9302)

System security is enforced by having credentials for IMPAX internal processes contained within encrypted password files that must be distributed to all server machines in the cluster.

IMPAX 6.5.1 sets up various user accounts for the IMPAX services. These accounts are set up with a random alphanumeric password, different for each installation. The passwords are encrypted with a key specific to the machine, and stored locally in a password file. The file cannot be copied to another system and decrypted.

To facilitate sharing information among servers, a passkey utility is used to export the password key into a portable format that can then be copied to another machine and imported. This portable file is encrypted during the export and secured with a password; the portable file is imported into another system by using the same password.

Differences between system and portable password files

(Topic number: 6936)

Two files contain IMPAX password information:

- System password file

  This file is encrypted with a key specific to the machine and unknown to the user, called the *system key*. This file is not transferable between machines and can be decrypted only on the system where it was created. It is located under the mvf directory and is named mvf.psd by default.

  Note:

  If the mvf.psd file already exists, do not remove it; otherwise, IMPAX services cannot start.

- Portable password file

  This file is encrypted with a key specified by the user, thus having a much weaker type of encryption. It is created upon user request, and should be deleted when no longer required. This key can be used to transfer passwords between systems during the installation of IMPAX.

Passkey utility reference

(Topic number: 6937)

To facilitate sharing information among servers, a passkey utility is used to export the password key into a portable format that can then be copied to another machine and imported. This portable file is encrypted during the export and secured with a password; the portable file is imported into another system by using the same password.

The passkey utility is in the /usr/mvf/bin directory on Solaris and the C:\mvf\bin directory on Windows. The command can be used in various modes, specified by the -M option. The -p and -r options allow you to specify non-default file names for the system password file and portable password file.

The command syntax is as follows:

passkey -M *mode, arguments* [**-p *file_name***] [**-r *file_name***]

where:

-M *mode*	**Arguments**	**Description**
CHECKKEY	**-k *user_key*** specifies the user key to check	This mode validates the user key against a portable password file.

-M *mode*	Arguments	Description
CREATE	**-u *username*** specifies which user to associate with the new password in the password file	This mode creates random, machine-specific passwords for users. Specify the user name for whom the password will be created, and optionally specify the name of the file to store the password in with the -p option.
DEC	**-S *source_string*** string to decrypt **-k *user_key*** key to use to decrypt machine	This mode is used for base64 decoding and decrypting a string. The encryption/decryption mechanism uses a system-specific key, meaning that the string cannot be decrypted on another machine. It can be decrypted only on the system where it was originally encrypted.
ENC	**-S *source_string*** string to encrypt **-k *user_key*** key to use to encrypt machine	This mode is used for base64 encoding and encrypting a string. The base64 encoding ensures the encrypted string is in ASCII format so that it can be stored in a text format. The encryption/decryption mechanism uses a system-specific key, meaning that the string cannot be decrypted on another machine. It can be decrypted only on the system where it was originally encrypted.
EXPORT	**-k *user_key*** specifies the key to use when creating the portable password file	This mode decodes the password file using the machine-specific key, and re-encodes it into a portable password file using the specified password (user key). This portable password file can then be copied to a new system and imported (see IMPORT) using the same specified user key.
IMPORT	**-k *user_key*** specifies the key used to create the portable password file	This mode decodes the portable password file using the user key, and re-encodes it into a password file with a machine-specific key. Creates an encrypted password file.
QUERY	**-u *username*** specifies which user to query for	This mode queries for a password associated with a given user name. The passkey utility writes the password to stdout (standard output). Typically, this function determines what password to set up for an account on a NAS server, which will allow the IMPAX components to connect.
SET	**-u *username*** specifies user to associate the password with **-P *password***	This mode sets the password for a given user to the password specified. This is used in cases where a random password is not suitable.

-M *mode*	Arguments	Description
	specifies password to associate with user	

VALIDATE	**-u *username***
	username to use in strong password validation
	-P *password*
	validates password against strong password encryption rules (used by Solaris installer)
		This mode can be used to test a specific password against strong password rules. A strong password must:
		• Be at least eight characters long
		• Not contain three or more characters from the user's account name
		• Contain characters from at least three of the following five categories:
		  • Uppercase (A to Z)
		  • Lowercase (a to z)
		  • Digits (0 to 9)
		  • Non-alphanumeric (for example, !, $, #, or %); avoid commas
		  • Unicode

-p *file_name*

optionally specifies a system password file name other than the default C:\mvf\mvf.psd (AS300) or usr/mvf/mvf.psd (AS3000)

-r *file_name*

optionally specifies a portable password file name other than the default C:\mvf\mvf.portable.psd (AS300) or usr/mvf/mvf.portable.psd (AS3000)

CAUTION!

The mvf.portable.psd file contains sensitive information. To maintain the security of the system, the portable password file should be deleted from both the Database Server and the target server locations after all new Network Gateway, Archive Server, Application Server, and Curator components are installed.

External software licenses

(Topic number: 7744)

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)

Copyright 1992 Simmule Turner and Rich Salz. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California. Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it freely, subject to the following restrictions: 1. The authors are not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it. 2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation. 3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation. 4. This notice may not be removed or altered.

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995-2003 International Business Machines Corporation and others. All rights reserved.

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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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 NON INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

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

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

all-in-one configuration

A configuration in which the Database, Archive Server, Network Gateway, and Curator Server components are all installed on a single Windows server, along with the Application Server software.

APIP

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

Application Server

Intermediary server between IMPAX Client and IMPAX Server machines. LDAP, Documentation, and other Business Services reside on the Application Server.

Autopilot

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

C

cc objects

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

CLUI

Command Line User Interface. A command-line tool to help in the service of IMPAX MVF. CLUI allows you to execute SQL statements.

cluster

A networking solution combining two or more otherwise independent computers, enabling them to work together in managing hospital data.

C-MOVE

An operation that allows an application entity to instruct another application entity to transfer stored SOP Instances to the original application entity or to a third application entity, using the C-STORE operation.

compression

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

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.

C-STORE

The mechanism used to transfer SOP Instances between application entities.

Curator

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

D

database

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

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.

E

external PACS archive

A PACS archive that resides outside the IMPAX cluster.

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

high availability

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

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.

HSM

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

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.

image

A single frame taken by a modality. Certain modalities, such as a CT, MRI, or PET, take consecutive sets of images called *series*. *Studies* are combinations of series or images for a single patient.

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.

logical volume

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

M

MAC address

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

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.

multi-host configuration

Server configuration in which the Database is installed on a separate computer from the Archive Server. Network Gateway may be installed on yet another server, or it may be installed along with the Database or Archive Server (or both).

multiple IMPAX cluster configuration

In a multiple IMPAX cluster configuration, an IMPAX cluster is linked to one or more other IMPAX or external PACS clusters, such that patient and study data can be shared and synchronized between them.

MVF_SCU

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

On IMPAX systems, it runs on the Network Gateway.

N

NAS

Network Attached Storage. A storage device attached directly to a Storage Area Network (SAN) or other direct network connection.

Network Gateway

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

O

OCR

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

ODBC

Open Database Connectivity. A standard protocol for accessing relational databases based around SQL.

P

PACS

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

PACS Store and Remember archive

An IMPAX server computer set up with the PACS Store and Remember archiving functionality. This server usually has Network Gateway functionality.

PAP

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

R

RIS

Radiology Information System. Responsible for scheduling exams and for report management in the Radiology department.

S

SAN

Storage Area Network. A network of shared storage devices. In a Storage Area Network, all storage devices are available to all servers on a Local Area Network.

SCP

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

SCU

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

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.

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.

V

volume

A volume refers to the division of data on the media. For example, if a tape has two sides, each side is referred to as a separate volume.

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.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z