AS3000 Upgrade and Migration Guide

IMPAX 6.2 or later to IMPAX 6.5.1

Upgrading an IMPAX 6.2 or Later Cluster

to an IMPAX 6.5.1 AS3000 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 186).

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 upgrade IMPAX, servers must meet certain hardware and software requirements.

Valid IMPAX upgrade paths

(Topic number: 6607)

Sites can upgrade to IMPAX 6.5.1 from any of these versions of IMPAX (supported versions include any applicable SUs):

- IMPAX 5.2.5—hereafter referred to as IMPAX 5.2
- IMPAX 5.3.1, 5.3.2—hereafter referred to as IMPAX 5.3
- IMPAX 6.2.1—hereafter referred to as IMPAX 6.2
- IMPAX 6.3.1—hereafter referred to as IMPAX 6.3
- IMPAX 6.4
- IMPAX 6.5

For more detailed information, refer to the *IMPAX 5.x - 6.x Service Update and Hot Fix Migration Paths* spreadsheet in the "Additional documents" section of the IMPAX Knowledge Base > Main Knowledge Base Page.

Important!

We recommend checking the migration log file after each leg of an upgrade before moving onto the next leg.

Additional information:

- AS3000 (Solaris) servers can upgrade to IMPAX 6.5.1 from any of the previously mentioned versions of IMPAX on Solaris 9 or 10. Existing Solaris 9 servers must upgrade to Solaris 10 when upgrading to IMPAX 6.5.1.
- Windows Server 2008 and Windows Server 2003 are supported on IMPAX AS300 servers. Windows 2008 is supported for fresh installations only; unless already on Windows 2008, Windows 2003 must continue to be used for upgrades.
- For IMPAX AS300 upgrades, SQL Server 2008 is supported.
- To upgrade an IMPAX AS300 cluster from SQL Server to Oracle, contact Agfa Professional Services for assistance. The SQL Server to Oracle migration process is not documented in this guide.
- The Application Server platform is either Windows Server 2003 or Windows Server 2008. Windows 2008 is supported for fresh installations only; unless already on Windows 2008, Windows 2003 must continue to be used for upgrades. All Application Servers in a cluster must use the same operating system—either Windows 2003 or Windows 2008.
- A site running IMPAX 4.5 can migrate its user data—passwords, IDs, and most preferences—to IMPAX 6.5.1. However, database data cannot be upgraded directly from IMPAX 4.5 to IMPAX 6.5.1. The IMPAX 4.5 database must first be upgraded to IMPAX 5.2.5, then to IMPAX 6.5.1.

Related documentation: IMPAX upgrades

(Topic number: 60109)

This guide is intended for service and administrative personnel who are upgrading an IMPAX 6.2 or later cluster to IMPAX 6.5.1. It is a companion volume to the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 6.2 or later to IMPAX 6.5.1*, which describes all tasks to be done leading up to the upgrade weekend. This guide covers the tasks to be done *during* the upgrade weekend. This includes how to upgrade the Database Server, and all other servers and clients at that same cluster.

If installing and initially configuring a new AS300 cluster, rather than upgrading an existing cluster, refer to the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*. For new AS3000 clusters, refer to the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

For information about using the IMPAX 6.5.1 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*.

IMPAX hardware and software requirements

(Topic number: 61303)

For optimal performance, Agfa recommends particular hardware and software for each component of the cluster.

IMPAX Application Server hardware and software requirements

(Topic number: 6682)

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

IMPAX Application Server: Hardware requirements

(Topic number: 6691)

The following hardware configuration is recommended for Application Servers.

Important!

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

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

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

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

IMPAX Application Server: Software requirements

(Topic number: 6621)

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

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

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: Non-SCSI CD/DVD burner and controller cards
(Topic number: 58044)

OEM-supplied CD/DVD writer

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: 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 Symmetrix DMX series Centera Centera Universal Access	StorageTek (STK)	D series B series

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

IMPAX AS3000 Server hardware and software requirements

(Topic number: 6675)

The following lists the hardware and software requirements for an IMPAX AS3000 Server. Where a specific manufacturer is identified, only that manufacturer's device is supported.

IMPAX AS3000 Server: Supported hardware configurations
(Topic number: 6689)

The four general categories of servers are:

- Single-host server—Database Server/Archive Server/Network Gateway
- Database Server hosting the Oracle database
- Archive Server or combined Archive Server/Network Gateway
- Network Gateway

The hardware requirements for each of these are outlined in the sections that follow.

IMPAX AS3000 Server: Hardware requirements
(Topic number: 6622)

We recommend the following components for each AS3000 server:

Component	Requirements
Validated systems	The following Sun servers can be used in any combination as required: For new installations: • T5120, T5220, T5140, T5240 For upgrades: • V240/V440 or newer • T2000, T5120, T5220, T5140, T5240 **Solaris 10u8 or later only.** We do not recommend Sun T1000, V210, and V215 because of the single power supply limitation. When planning upgrades, note all end-of-sales and end-of-support dates published on MedNet. **Note:** These servers must have a DVD-ROM drive present for IMPAX installation purposes.
Number of CPUs	A minimum of two CPUs should be used in any of the server categories, after which the number of CPUs should be determined by server usage. General recommendations: • Database Server: Two to six CPUs • Archive Server/Network Gateway: Two to four CPUs • Network Gateway: Two CPUs

Component	Requirements
	• Single-host server: Two to eight CPUs Does not apply to the multi-core processors used in T-series Sun servers.
RAM	A minimum of 2 GB per CPU should be used in any of the server categories, after which the amount of RAM should be determined by server usage. General recommendations: • Database Server: 2GB per CPU • Archive Server/Network Gateway: 2GB to 4GB per CPU • Network Gateway: 2GB to 4GB per CPU • Single-host server: 2GB to 8GB per CPU
Hard drive	A minimum of two hard drives should be used in any of the server categories, after which the number of drives should be determined by server usage and configuration. We recommend having data available on an external disk subsystem and not an internal drive.
RAID	Required • RAID 1 + 0 is mandatory for the database (along with ForceDirectIO)—See the partitioning recommendations in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*. • RAID 5 or better for image cache.
Tape backup	Optional for Database Server but not recommended—not required if using file system backups.
Modem	Not required.
DVD-ROM	Required—One per cluster is required.
Floppy	No.
Network interface	Sun 10/100/1000 Mbps NICs. A 1 gigabit network should be considered the minimum for server interconnections. Consider segregating network traffic in order to improve overall throughput.
Jukebox	Direct attached archives are not supported.
Other	UPS that meets the region's safety approval standards and the power requirements of the machines it supports.

IMPAX AS3000 Server: Database backup requirements
(Topic number: 10319)

For file system backup, the following are supported:

- Back up to NFS or SAN

For tape backup (upgraded systems only, not new installations), the following are supported:

- SUN DAT-72
- Standalone DLT 8000
- Standalone LTO2
- Standalone SDLT
- Standalone L8 with LTO or LTO2 or SDLT

Important!

Oracle disk-to-tape backup requires significant disk space, as a minimum of two backups must be kept on disk. To accommodate disk-to-tape backups of the Oracle database, ensure that you define a Flashback partition that is at least 3 times the expected size of the database.

Operating systems disks should be configured as RAID 1, preferably with hardware mirroring; however, on platforms that do not support hardware mirroring, Solstice DiskSuite is acceptable. For more information regarding disk management strategies, refer to "Disk management strategies" (topic number 103117) in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

IMPAX AS3000 Server: External storage requirements
(Topic number: 10321)

When planning upgrades, note all end-of-sales and end-of-support dates published on MedNet. A comprehensive list of currently supported storage products is available through Agfa Professional Services.

For external storage, the following are supported:

EMC CX Series

EMC DMX series

EMC NS NAS

HP EVA series

HBAs supported by storage vendor and operating system

IMPAX AS3000 Server: Software requirements
(Topic number: 6620)

The following software is required for an IMPAX AS3000 cluster:

Component	Requirements
Operating system	Solaris™ 10u8 or later.
Database software	Oracle 10.2.0.4.0 Standard or Enterprise Editions (supplied with IMPAX)
Solaris patches	As recommended by Sun.

Component	Requirements
Other software	• Java Runtime (included with Solaris) • Apache Server (included with Solaris) • Adobe® Reader® for Solaris (for documentation)
Supported software	The following software is supported but not required: • SUN SAM-FS 4.5/4.6/5.0 on Solaris 10, NFS or local • IBM Tivoli Storage Manager—NFS only • QStar • EMC Centera

Curator hardware and software requirements

(Topic number: 6714)

We recommend the following hardware and software for a dedicated Curator and CD Export server.

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

Component	Requirements
	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.

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)

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

IMPAX Client hardware and software requirements

(Topic number: 6679)

The following lists the recommended hardware and software for an IMPAX Client workstation.

IMPAX Client: Hardware requirements

(Topic number: 7793)

The following hardware configuration is recommended for new workstations. While IMPAX Client should work on an equivalent platform, optimal results can be guaranteed only on the recommended platform.

To use the CT-MR navigation tools, we strongly recommend that, due to the high volume of data being manipulated, Client systems be equipped with a high-end video subsystem that is PCIe X16 based.

CAUTION!

For official diagnostic interpretation, we recommend setting the display to 32-bit color or more.

Component	Requirements
System	The Agfa preferred supplier is HP. HP xw4400, xw4600, xw6400, xw6600, z400, or z600 Dell Precision™ 490 or 690, T5400, T7400, or T7500 Motion LE1600 Tablet PC (Non-diagnostic)
CPU	2 x 2.0GHz or higher 1 x Dual/Quad Core 2.8GHz or higher

Component	Requirements	
	1 x Intel® Pentium® M 1.5GHz (Tablet PC – Non-diagnostic)	
RAM	Windows XP: 1 GB minimum Windows Vista and Windows 7: 4 GB minimum 4 GB recommended for all new systems for optimal performance and viewing of large volume image sets 4 GB recommended for IMPAX Clinical Applications such as IMPAX Virtual Colonoscopy, IMPAX PET-CT Viewing, and IMPAX Reporting (embedded speech recognition)	
RAM (Tablet OS)	512 MB min (Non-diagnostic Tablet PC only)	
Hard drive space	80 GB minimum	
Modem	Not applicable	
DVD-ROM drive	Yes	
Floppy drive	Not applicable	
Network interfaces	System comes with an integrated 100/1000 Mbps Ethernet adapter	
Power supply	Default	
Peripherals	Scroll mouse and keyboard For North America, the Logitech MX518 is used with the MA3000.	
Other	Microsoft supported DVD RW/CDRW	
Video		
Diagnostic review workstations and high-end diagnostic review workstations	**Windows 7 (WDDM)*:** MXRT1150, 2150 MXRT5200 (covers 98% of the diagnostic requirements) MXRT7200 (high end board for IMPAX Clinical Applications such as Oasis for IMPAX) MXRT7300 (high end board for IMPAX Clinical Applications such as Oasis for IMPAX. Supported from WDDM v1.1 May/June 2010)	**Windows XP and Vista:** BarcoMed PCIe for Coronis BarcoMed PCIe for Nio BarcoMed PCIe 5MP2FH (only with monitor MF GD-5621HD) MXRT 2100/5100/7100 (not sold anymore but still supported) MXRT5200 (covers 98% of the diagnostic requirements) MXRT200 and 7300 (high-end board for IMPAX Clinical Applications such as Oasis for IMPAX)
RIS/Administrator stations and Clinical review stations	**Windows 7 (WDDM):** NVIDIA FX 1700, FX 1800, FX 4800	**Windows XP and Vista:** NVIDIA FX 1700, FX 1800, FX 4800

Component	Requirements	
	ATI 3700, 3750, V3800 (third monitor board)	ATI 3700, 3750, V3800 (third monitor board)
	MXRT 1150/2150 (third monitor board)	MXRT 1150/2150 (third monitor board)

*Windows 7 and WDDM drivers do not support the BarcoMed and older MXRT (2100, 5100. and 7100) boards.

IMPAX Client: External software requirements

(Topic number: 6694)

The following software is required for all new stations. Unless otherwise indicated, Agfa does not provide the software as part of the IMPAX Client installation package.

Component	Requirements
Operating system	Microsoft Windows XP Professional SP3 may be used for upgrades but is no longer available for shipment
	Microsoft Windows Vista™ / Windows Vista x64 (Business and Ultimate) SP2
	Windows 7 Professional 64-bit (single language support), Windows 7 Ultimate 64-bit (multi-language support) SP1 for Diagnostic review stations
	Note that other versions of Windows 7 can be used for non-diagnostic review stations.
Other software	Microsoft Internet Explorer 7.0 and 8.0
	.NET 3.5 SP1
	Latest version of Adobe® Reader®
	Antivirus software such as Norton Antivirus 6.1 or higher, Trend Micro, or McAfee Antivirus 4.5 or higher
	Note that Oracle 11 Client is required for IMPAX Reporting and IMPAX for Cardiology.

The IMPAX Client will run on 64 bit operating systems in 32bit compatibility mode. The IMPAX Client is not a 64bit application and therefore does not take advantage of 64bit processing or memory addressing.

Note:

We recommend upgrading Windows Vista to Windows 7 for systems that will be used as diagnostic workstations.

Preparing to upgrade

2

Important!

Before proceeding with the upgrade of the AS3000 server components, ensure that you have completed the tasks, including installing the IMPAX 6.5.1 Migration Toolbox, outlined in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 6.2 or later to IMPAX 6.5.1*.

Before upgrading from an IMPAX 6.2 or later cluster to an IMPAX 6.5.1 AS3000 configuration, you must complete certain preparatory tasks, such as taking a system snapshot, stopping the transmission of data to IMPAX 6.2 or later, redirecting studies to the traveling server, and halting queues.

1. Gathering information and equipment

(Topic number: 6884)

Before performing the AS3000 server upgrade and migration, gather the information and equipment needed when migrating and upgrading the stations.

IMPAX 6.2 or later upgrades: Necessary information and equipment

(Topic number: 10130)

Equipment and information	Notes
Whether the Cross-Cluster Dictation Interlock tool needs to be run	
Which version of Solaris is being used: Solaris 9 or Solaris 10	
A Solaris maintenance agreement and login details, for installing patches	
Whether Oracle Data Guard is being used	

Equipment and information	Notes
If upgrading Windows-based Archive Servers or Network Gateways, Windows Server 2003 R2 Service Pack 2 or Windows Server 2008 Service Pack 2	
Whether adding an Audit Record Repository to the cluster	
Whether a traveling server is being used	
Which time server to synchronize with	

2. Running the Cross-Cluster Dictation Interlock tool

(Topic number: 47379)

Before it can be run, the Cross-Cluster Dictation Interlock tool must be installed and configured. Refer to "Installing and running the Cross-Cluster Dictation Interlock tool" (topic number 48033) in the appropriate version of the *IMPAX Preparing to Upgrade Guide*.

The Cross-Cluster Dictation Interlock tool synchronizes both the dictation status and the claim status of studies between the previous version of IMPAX and IMPAX 6.5.1, when these are running in parallel—such as may happen when using a training server, when using a traveling server (AS3000 sites), or if planning to run the upgraded IMPAX cluster alongside the previous-version IMPAX cluster for a transition period.

Note:

Synchronization of the claim status of studies occurs only between versions of IMPAX that support shared workflows from which radiologists can then claim ownership of studies.

To run the Cross-Cluster Dictation Interlock tool

1. On the 6.5.1 Application Server where the Relay service is running, open a command prompt.
2. Type the following command:

   net start StudyStatusRelayService
3. Exit the command prompt.

3. Taking a pre-migration system snapshot

(Topic number: 6844)

Before upgrading to IMPAX 6.5.1, use the migration_inventory tool to capture the current state of the system for later comparison. Perform this task on any computer with access to the AS3000 database and on which the Migration Tools have been installed.

To take a pre-migration system snapshot

1. Log in as mvf.
2. In a terminal window, change to the directory containing the migration_inventory tool.
3. Type

   ./migration_inventory -s -d *database_name* -U *database_user_name* -P *database_password* -D *Database_Server_host_name*

   The output is stored in the migration_info table. It lists the number of IMPAX studies, total objects, and objects in cache. It also lists all IMPAX source stations and DICOM printers.
4. To create a report file with this information, type

   ./mig-reporter -t system_inventory_tool

   This command writes the output of the migration_inventory command to a report file in the /usr/mvf-mig6/reports directory. (For other parameters you can use with this command, refer to the "mig-reporter" reference topic, topic number 10635, in the appropriate version of the *IMPAX Preparing to Upgrade Guide*.)

Tip:

For ease of reading this report, you can open it in Microsoft Excel, if you have access to this program.

4. Emptying Connectivity Manager queues

(Topic number: 113307)

You can manage queues through Service Tools, which is the Connectivity Manager interface. Service Tools consists of a series of Managers. The Queue Manager displays a list of devices with queues, and provides queue management functionality.

Before shutting down IMPAX to upgrade the system, empty all DM Out or impax_report_server queues. Consult Connectivity Manager service personnel to discuss queues that have error transactions.

To empty Connectivity Manager queues

1. In Connectivity Manager, open Service Tools and click **Queue Manager**.
2. Select any device with either pending or error transactions and empty the queues.
3. Retry recent messages and delete older messages since newer transactions may have updated patient, study, and report data after these transactions entered an error state.

5. Stopping Connectivity Manager interfaces

(Topic number: 113766)

During the IMPAX upgrade, you can prevent the loss of clinical patient updates from hospital information systems by stopping data bound for the Connectivity Manager, or by stopping the Connectivity Manager's outbound queues. The preferred method is to stop inbound interfaces, which prevents the Connectivity Manager from receiving incoming messages.

Coordinate with hospital information system personnel to confirm that they are capable of holding messages in queues. If the information system queues can be stopped, also stop the Connectivity Manager's inbound interfaces.

To stop Connectivity Manager interfaces

1. In the Connectivity Manager, open **Service Tools**.

   The Device Manager displays a list of devices and interfaces and their status.
2. To resort and group all device classes, click **Class**.
3. Scroll down to view CMSI and HL7 class devices.
4. Note which **HL7 In** and **CMSI In** interfaces are started. These interfaces must be restarted after the IMPAX upgrade.
5. Select the checkbox beside each of the started inbound interfaces.
6. Click **Stop**.

The status of each selected interface changes to Stopped.

6. Stopping Connectivity Manager queues

(Topic number: 67550)

If the Connectivity Manager's inbound devices have not been stopped, stop the IMPAX outbound DM Out and impax_report_server queues prior to shutting down IMPAX for the upgrade. Messages in stopped queues are not processed and remain in the queue until the queue is restarted. Outbound queues are restarted automatically if the Agfa Connectivity service is restarted, or if the Connectivity Manager is rebooted.

To stop Connectivity Manager queues

1. In the Connectivity Manager, open **Service Tools** and click **Queue Manager**.
2. In the Queue List table, select the checkbox beside each queue belonging to a device with a DM Out or impax_report_server component.
3. Click **Stop**.

   The status of the queues changes to Stopped.

Connectivity Manager outbound message queues must be configured with the new server settings before messages are added to the queues. Consult a Connectivity integrator to create a device for the destination IMPAX server. Report updates can be sent to only one IMPAX server, after all reports have been copied to that server. This applies to the traveling server, if used, and also the migrated IMPAX server.

7. Updating study status between servers

(Topic number: 51514)

Important!

This topic applies only when using an AS3000 traveling server as part of the upgrade and migration.

When studies are dictated on the production server, a delay occurs before the traveling server is updated with the new status. Due to this delay, when switching to the traveling server during the migration process, some studies that have already been dictated will switch back to status `New`. To avoid this problem, synchronize the study status before redirecting studies to the traveling server.

To update study status between servers

1. Log in as oracle user on the production Database Server, log into sqlplus as **dbadmin** and type

   create public database link travel connect to dbadmin identified by *admin_password* using '*traveling_server_name*';

   where *admin_password* is the password for the dbadmin user on the traveling server and *traveling_server_name* is the name of the traveling server.

2. In a text editor such as vi, edit the /var/opt/oracle/tnsnames.ora file to add the traveling server.

```
traveling_server_name.world =
 (DESCRIPTION =
     (ADDRESS_LIST =
         (ADDRESS =
            (COMMUNITY = impax.world)
            (PROTOCOL = TCP)
            (Host = traveling_server_name)
            (Port = 1521)
         )
     )
     (CONNECT_DATA = (SID = MVF)
     )
)
```

3. Perform the report status update by typing the following into sqlplus:

   declare

   the_counter number := 0;

   cursor study_cursor is

   select t.study_ref, s.status from dosr_study s, dosr_study@travel t

where s.patient_id = t.patient_id and s.accession_number = t.accession_number

and s.status <> t.status;

begin

for study_record in study_cursor LOOP

update dbadmin.dosr_study@travel set status = study_record.status where study_ref = study_record.study_ref;

the_counter := the_counter +1;

if mod (the_counter, 100) = 0 then

commit;

end if;

end loop;

commit;

end;

/

4. Drop the link to the traveling server database by typing the following in sqlplus:

   drop public database link travel;

8. Redirecting studies to the traveling server

(Topic number: 60448)

Important!

This topic applies only when using an AS3000 traveling server as part of the upgrade and migration.

Configure the modalities to redirect studies to traveling server, so that they remain accessible while the migration continues. How studies are redirected is modality-specific and is not documented in this publication.

9. 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).

Use the information from the latest report on archiving studies to identify remaining unarchived studies (for details, refer to the appropriate version of the *IMPAX Preparing to Upgrade Guide*). 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 6.2 or later 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: 58298)

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

To store unarchived studies

1. In the 6.2 or later 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.

Note:

To store unarchived studies, you could also use the Migration Toolbox and run the study_archive_report tool. Refer to the “Running an initial report on study archiving status” topic in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 6.2 or later to IMPAX 6.5.1*.

10. Stopping SMMS server alerts

(Topic number: 10136)

If using an SMMS (PACSWatch) server, prevent it from sending alerts before shutting down IMPAX, so that the GSC (Global Support Center) does not get false alerts.

To stop SMMS server alerts

1. On the SMMS server, double-click the **Disable GSC Notifications** icon.
2. Open the **C:\agfa\config\emailcmd.cfg** file for editing.
3. Change the line `enabled = 'true'` to **enabled** = **'false'**.
4. Save the file and close it.

Alerts are no longer sent about that server, but the rest of the system continues to be monitored.

11. Dropping Heartlab triggers

(Topic number: 60542)

This topic is applicable to Heartlab-integrated systems only.

Drop the Heartlab triggers before upgrading the database.

To drop Heartlab triggers

1. On the Database Server, log in as oracle user and using SQLPLUS, log in as user **dbadmin**.
2. Type the following:

   `SQLPLUS>` **drop trigger TRG_DOSR_STUDY_UPD;**

   `SQLPLUS>` **drop trigger TRG_DOSR_SERIES_UPD;**

   `SQLPLUS>` **drop trigger TRG_DOSR_OBJECT_UPD;**

   `SQLPLUS>` **exit;**

12. 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.

13. Shutting down the IMPAX system

(Topic number: 10140)

All components of the IMPAX system must be shut down before upgrading the database software.

Stopping all queues

(Topic number: 60451)

Allow remaining SEND jobs to continue until they have finished, then stop any more studies from moving around the IMPAX system.

To stop all queues

1. Launch the Administration Tools and log in as the **administrator** user.
2. On the Daily tab, select **Job Manager**. 
3. Select **All Queues**.
4. Click **Halt Queue**. 

All queues are now halted.

Stopping services on the Application Servers

(Topic number: 10144)

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

To stop services on the Application Servers

1. On an Application Server, open the Windows Administrative Tools and select **Services**.

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

Stopping IMPAX services on AS300 servers

(Topic number: 10146)

If using an AS300 (Windows-based) Network Gateway or Archive Server in a mixed-host configuration or an IMPAX Curator in any configuration, you must stop IMPAX services on these servers before upgrading the AS3000 Database Server.

To stop IMPAX services on AS300 servers

1. On an AS300 server, in Windows Explorer, navigate to C:\mvf\bin.
2. Double-click **stopall.bat**.
3. Double-click **removeall.bat**.

This stops then removes IMPAX services from that server. Repeat for each AS300 server.

Stopping IMPAX on AS3000 servers

(Topic number: 10150)

You must disable IMPAX on each IMPAX AS3000 server, including any IMPAX 6.5.1 servers that you have staged in advance.

Important!

Perform this task on any Archive Server or Network Gateway servers first, then on the Oracle Database Server.

To stop IMPAX on AS3000 servers

1. Log into the AS3000 server as the **root** user.
2. To stop IMPAX, type

    stop_impax
3. Then type

disable_impax

`No such file or directory` error messages may be displayed. You can safely ignore them.

This stops then disables IMPAX on that server.

14. Disabling IMPAX crontab entries

(Topic number: 10152)

If Oracle processes such as database backup, task scheduler, or database analysis start to run while Oracle is being upgraded, the database will be damaged. To prevent this from happening, comment out any entries in crontab that would launch such processes.

To disable IMPAX crontab entries

1. Log into the Database Server as the **mvf** user.
2. To open the crontab file, type **crontab -e**.
3. Check the file carefully for any entries related to IMPAX.
4. Comment out any IMPAX entries that you find.
5. Save and close the file.

15. Stopping CLUI and ISQL

(Topic number: 6848)

You must stop CLUI and ISQL before upgrading the database. If either application is running, the automated upgrade script cannot continue. The Oracle installation fails and leaves the database in an unusable state.

Checking for the CLUI and ISQL processes

(Topic number: 58303)

Check whether the CLUI and ISQL processes and need to be stopped before the upgrade.

To check for the CLUI and ISQL processes

1. Log into the Database Server as the **mvf** user.
2. Type

   psg clui

   psg isql

   If these processes are not running, nothing is returned.

   But if either process is running, you see the row of headers along with a row of data; for example:

```
USER PID %CPU %MEM SZ RSS TT S START TIME COMMAND
mvf 26409 3.2 4.8 3518 1184 pts/7 T 13:12:53 0:00 clui
```

3. If processes are running, record the PID number from the returned header.

Stopping the CLUI and ISQL processes

(Topic number: 58306)

If the CLUI and ISQL processes are running, stop them before the upgrade.

To stop the CLUI and ISQL processes

1. Log into the Database Server as the **mvf** user.
2. Type

   kill -9 *PID_number*

   For the PID, look in the output of the previous procedure. In the preceding example, the PID is 26409.

Ensuring that the CLUI and ISQL processes are stopped

(Topic number: 58309)

After stopping CLUI and ISQL, verify that they are no longer running.

To ensure that the CLUI and ISQL processes are stopped

1. Log into the Database Server as the **mvf** user.
2. Type

   psg clui

   psg isql
3. Ensure that nothing is returned.

16. Shutting down the Database Server

(Topic number: 10156)

Run these commands on the Database Server before upgrading the software or restaging the server.

To shut down the Database Server

1. Log into the Database Server as the **mvf** user.

   or

   When restaging a Database Server already running Oracle 10.2.0.4.2, log in as the **oracle** user.
2. To shut down the database, type

dbshutmvf

3. To shut down the listener, type

   lsnrctl stop

4. To confirm that all IMPAX and Oracle processes have stopped, type

   psg mvf

   psg ora

   psg tns

5. Verify that, in each of these cases, nothing is returned.

17. Storing a cold backup of the database and other Oracle configuration files

(Topic number: 59281)

Back up the Oracle data and configuration files immediately before the start of the upgrade or restage. This procedure can take a significant amount of time. To estimate how long it will be, check the duration of warm backups as recorded in the /data/logs/backup.log file.

To store a cold backup of the database and other Oracle configuration files

1. If using a NFS share to store the backup, start the NFS service on the server where the backup files will be stored.

   On Solaris 10, type

   su -

   svcadm -v enable -r network/nfs/server

   or

   On Solaris 9, type

   su -

   cd /etc/rc3.d

   ./s15nfs.server start

2. To share the directory that the IMPAX server will be writing to use a Unix text editor such as vi. For example, type

   su -

   vi /etc/dfs/dfstab

3. Add the following line

   share -F nfs -o rw,anon=0 ***path_to_backup_location_directory***

4. Save and close the file.

5. On the IMPAX server, mount the share as the **root** user. For example, type

mkdir /*backup_location*

mount -o rw,bg,hard,rsize=32768,wsize=32768,vers=3,forcedirectio,nointr,suid *server_containing_backup*:*absolute_path_to_backup_location_directory* /*backup_location*

6. As the **root** user, copy the appropriate files to the backup location.

Original directory	File	IMPAX 6.5.1 directory	Description
/dbase	all files under this directory	/dbase	Oracle data files and control files
/usr/oracle/current/dbs or /opt/oracle/current/dbs (if replacing an IMPAX 6.4 or later server)	orapw	/opt/oracle/current/dbs	Oracle password file location
	initMVF.ora		Oracle text initialization parameter file
	spfileMVF.ora		Oracle binary initialization parameter file (only if running Oracle 10.2)
	dr1MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
	dr2MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
/var/opt/oracle	tnsnames.ora	/var/opt/oracle	Oracle Naming Configuration
	listener.ora		Oracle Listener Configuration
	sqlnet.ora		Oracle SQLNET Configuration
	listener.ora.dg*xx*		IMPAX 6.4 or later Oracle Listener Configuration backup

Original directory	File	IMPAX 6.5.1 directory	Description
	tnsnames.ora.dg*xx*		IMPAX 6.4 or later Oracle Naming Configuration backup
	tnsnames.ora.client		Oracle Listener Configuration for clients (only when Oracle Data Guard is configured)
/cache/mvfcache	all files under this directory	/cache/mvf/cache	IMPAX cache—only if the cache directory is physically on the Database Server
/usr/mvf	dg_info	/usr/mvf	Oracle Data Guard cluster information for IMPAX

For example:

cp -r /dbase /*backup_location*

cp -r /usr/oracle/current/dbs/orapw /*backup_location*

cp -r /usr/oracle/current/dbs/initMVF.ora /*backup_location*

cp -r /usr/oracle/current/dbs/spfileMVF.ora /*backup_location*

cp -r /usr/oracle/current/dbs/dr1MVF.dat /*backup_location*

cp -r /usr/oracle/current/dbs/dr2MVF.dat /*backup_location*

cp -r /var/opt/oracle/tnsnames.ora /*backup_location*

cp -r /var/opt/oracle/listener.ora /*backup_location*

cp -r /var/opt/oracle/sqlnet.ora /*backup_location*

cp -r /var/opt/oracle/listener.ora.dg*xx* /*backup_location* where *xx* is the IMPAX version

cp -r /var/opt/oracle/tnsnames.ora.dg*xx* /*backup_location* where *xx* is the IMPAX version

cp -r /var/opt/oracle/tnsnames.ora.client /*backup_location*

cp -r /usr/mvf/dg_info /*backup_location*

cp -r /cache/mvfcache /*backup_location*

18. Removing System DSN entries for Oracle ODBC drivers

(Topic number: 67668)

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

Before upgrading Oracle Server (and changing the Oracle home), remove the existing mvf and mvf_ora DSNs from all Windows-based servers, including any AS300 Archive Servers and Network Gateways, the Application Server, and Curator, but not on the IMPAX Client stations.

To remove System DNS entries for Oracle ODBC drivers

1. On the AS300 server or the Application Server, open the Windows Administrative Tools.
2. Select **Data Sources (ODBC)**.
3. Switch to the **System DSN** tab.
4. Select the **mvf** System Data Source.
5. Click **Remove**.
6. To confirm the removal, click **Yes**.
7. To save the changes and close the dialog, click **OK**.
8. On the Application Server, repeat the previous steps for the **mvf_ora** System Data Source as well.

19. Recording the names of previously installed IMPAX AS3000 software packages

(Topic number: 120768)

Before uninstalling the AS3000 server packages for the previous release of IMPAX, record the package names. It is useful to know these before installing IMPAX 6.5.1.

To record the names of previously installed IMPAX AS3000 software packages

1. Navigate to the /install_info file.
2. Open the file in a text editor.

```
ORACLE_VERSION='Oracle10.2.0.4.0'
SOLARIS_HW_REV=''
HOSTNAME='bigbird'
DOMAINNAME='mitra.com'
AE_TITLE='bigbird'
REPOSITORY='/export/impax_install'
```

```
REPOSITORY_USER='root'
REPOSITORY_HOST='127.0.0.1'
APPS_SERVER='matilda.aqua.mitra.com'
AGFA_SERVICE_ENCRYPT='3PM2kGd2Jn/0X2TFIoJ4/s4FH9qkkvD2RX4syckIppwUarOwpTcbxxMl0tsLdTfbwOQdtA=='
IPADDRESS='10.237.236.9'
ETHERADDRESS='0:3:ba:9:1a:33'
INSTALL_SERVER='127.0.0.1'
INST_ipaddress='10.237.236.223'
ORA_SERVER='y'
SERVER_HOST='bigbird'
ORA_ipaddress='10.237.236.9'
DLTBACKUP='n'
IMAGE_CACHE='y'
GATEWAY='y'
OCR='y'
LOSSY_JPEG='y'
JUKEBOX='dlt'
PAP='y'
STORAGE_ARRAY='n'
MODEM_TYPE='multitech'
MODEM_PRESENT='n'
SMARTUPS='n'
SYSTEM_INFO="V280R, 2xuSPARC-III@800MHz, 2x36GBx10kFC disks, 2GB RAM"
COMMENTS=""
```

3. Make note of the following entries (note that your entries may differ from the example):
   - ORA_SERVER='y'
   - IMAGE_CACHE='y'
   - GATEWAY='y'
   - OCR='y'
   - LOSSY_JPEG='y'
   - JUKEBOX='dlt'

Upgrading Oracle Server and the IMPAX database data and schema

3

Important!

Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

After completing all preparatory tasks, you can proceed with upgrading Oracle Server and the IMPAX database data and schema.

Note:

If upgrading an AS3000 cluster from IMPAX 6.5 to IMPAX 6.5.1, you can skip ahead to the *Upgrading an IMPAX 6.5 AS3000 cluster to IMPAX 6.5.1* (refer to page 68) tasks.

1. Increasing the tablespace size on Solaris

(Topic number: 6875)

If required, run the monitor_add script to add 2 GB of MVFL, MVFLINDX, MVF, MVFINDX, and UNDO tablespaces to aid the upgrade process.

Important!

For Oracle Data Guard servers, increase the tablespace size only on the primary Database Server.

To increase the tablespace size on Solaris

1. Log into the Database Server as the **mvf** user.
2. Start the database by typing

   dbstartmvf

   Note:

   If Oracle has already been upgraded, you can ignore the error `SQL> SP2-0310: unable to open file "/usr/oracle/current/rdbms/admin/dbmspool.sql"`, as long as the database is able to start.

3. Start the listener. Type

   lsnrctl start
4. Change to the **/usr/mvf-mig6/bin** directory.
5. To see whether 2–3 GB of space is available for the MVFL tablespaces, type

   /usr/mvf/bin/monitor_update

   /usr/mvf/bin/monitor_stats
6. If additional space is needed, to run the monitor_add script, type

   /usr/mvf/bin/monitor_add
7. To continue, type **C**.
8. Type the tablespace name, **MVFL**.
9. Type the path name for the data file.
10. Type the size of the file in megabytes, **2000**.

    The file is created.
11. Repeat these steps for the MVFLINDX, MVF, MVFINDX, and UNDO tablespaces, substituting the appropriate tablespace name each time.

2. Upgrading to Oracle Server 10.2.0.4.2

(Topic number: 6829)

The upgrade-oracle script upgrades Oracle Server from versions 9.2.0.4, 10.1.0.2, 10.2.0.2.0, 10.2.0.3.0, or 10.2.0.4.0 to Oracle 10.2.0.4.2.

You can upgrade Oracle either from the Oracle for Solaris DVD or by creating a repository to work from.

Tip:

If you are upgrading an Oracle Data Guard server, the following procedure does not apply and you can skip ahead to *Upgrading the primary Data Guard server to 10.2.0.4.2* (refer to page 44).

To upgrade to Oracle Server 10.2.0.4.2

1. Log into the Database Server as the **root** user.
2. If using a software repository that is not on the local machine, mount the repository.

   For example, if server1:/updates is the location of the repository, type

   mkdir /software

   mount server1:/updates /software

   Important!

   After mounting the repository, make sure to unmount the directories before proceeding any further. If the directories are not unmounted, the upgrade fails.

3. Change to the **/usr/mvf-mig6/bin** directory.
4. Type **./upgrade-oracle**.
5. To confirm that the latest patches have been applied, type

   $ORACLE_HOME/OPatch/opatch lsinventory
6. Type the path of the Oracle 10.2.0.4.2 software repository.

   For example, type ***/software_repository_path***
7. Type **y** when prompted to upgrade Oracle Server and when prompted to remove the existing Oracle package.
8. If the following error message appears:

   ```
   Unable to stop the cron process. Stop it manually as user root in /etc/init.d
   and execute ./cron stop before re-running this script.
   ```

   Manually disable the cron process. As the **root** user, type

   svcadm disable svc:/system/cron:default

   Note:

   Re-enable cron after the upgrade has completed. Type **svcadm enable svc:/system/cron:default**.

9. Type the path for the Oracle Flashback location.

   The Flashback location defines where backup data is stored.
10. Type the Flashback location size.

The upgrade may take over an hour to complete.

You can ignore the following errors:

- Any error messages regarding `mail: Invalid permissions on /var/mail/oracle`.

  These permissions are corrected during the upgrade.
- `Line 74: cat: cannot open /var/tmp/curver.out`
- `Line 103: ./upgrade-oracle: line 1170: log: command not found`

3. Upgrading the primary Data Guard server to 10.2.0.4.2

(Topic number: 67263)

Important!

This topic applies only when upgrading Oracle Data Guard servers.

Before running the upgrade script, ensure that Oracle has been started on both the primary and standby servers.

The upgrade-oracle-dg script upgrades an Oracle Data Guard server from version 10.2.0.2.0 to 10.2.0.4.2. You can upgrade Oracle either from the Oracle for Solaris DVD or by creating a repository to work from. Information about configuring Oracle Data Guard is available in the *IMPAX 6.5.1 Server Knowledge Base*.

Important!

Before proceeding with this upgrade, run the **check_standby** script on the primary Database Server to ensure that the Data Guard cluster is functioning correctly and that no archive gaps exist between the primary and standby servers. For more information, refer to "*Tools for monitoring Oracle Data Guard* (refer to page 166)" (topic number 66589) in the *IMPAX 6.5.1 Server Knowledge Base*.

To upgrade the primary Data Guard server to 10.2.0.4.2

1. Log into the primary Database Server as the **root** user.
2. If using a software repository that is not on the local machine, mount the repository.

   For example, if server1:/updates is the location of the repository, type

   mkdir /software

   mount server1:/updates /software

Note:

After mounting the repository, make sure to unmount all the repository directories before proceeding. If the directories are not unmounted, the upgrade fails.

3. Change to the **/usr/mvf-mig6/bin** directory.
4. Type **./upgrade-oracle-dg**.
5. Type the path of the Oracle 10.2.0.4.2 software repository.
6. Confirm that you are upgrading the *Primary Database*.

   You can ignore any error messages regarding `mail: Invalid permissions on /var/mail/oracle`. These permissions are corrected during the upgrade.

The upgrade may take over an hour to complete.

Once the upgrade has started, you can begin the standby Database Server upgrade. Both upgrades can run simultaneously.

4. Upgrading the standby Data Guard server to 10.2.0.4.2

(Topic number: 67758)

Important!

This topic applies only when upgrading Oracle Data Guard servers.

Once the upgrade of the primary Database Server has started, you can begin the standby Database Server upgrade. Both upgrades can run simultaneously.

To upgrade the standby Data Guard server to 10.2.0.4.2

1. Log into the standby Database Server as the **root** user.
2. If using a software repository that is not on the local machine, mount the repository.

Note:

After mounting the repository, be sure to unmount the directories before proceeding any further. If the directories are not unmounted, the upgrade fails.

3. Change to the **/usr/mvf-mig6/bin** directory.
4. Type **./upgrade-oracle-dg**.
5. Type the path of the Oracle 10.2.0.4.2 software repository.
6. Confirm that you are upgrading the *Standby Database*.

You can ignore any error messages regarding `mail: Invalid permissions on /var/mail/oracle`. These permissions are corrected during the upgrade.

The upgrade should not take as long as the upgrade of the primary Database Server.

If the `Database "MVF" possibly left running when system went down (system crash?). Notify Database Administrator.` error occurs, you can safely ignore it. The error occurs because the upgrade-oracle-dg script attempts to start the MVF database to check if the configuration is a Data Guard setup or not. The script at this point does not know about the configuration.

5. Upgrading the IMPAX 6.2 or later database data and schema to IMPAX 6.5.1

(Topic number: 60408)

Important!

Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

Upgrading the 6.2 or later database schema to 6.5.1 requires the IMPAX Migration Tools. For Migration Tools installation instructions, refer to the "Installing the IMPAX 6.5.1 Migration Toolbox" section in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 6.2 or later to IMPAX 6.5.1*.

During the schema upgrade, a MAP_EVENT_AUDIT.dmp file is created in the /usr/mvf-mig6/data directory. Ensure that enough space is available for this file: upwards of 10 GB, depending on the size of the database and the MAP_AUDIT_EVENT table.

CAUTION!

Any customization to the database—such as extra indexes, stored procedures, or triggers—may affect the schema upgrade. We recommend removing such customizations prior to the upgrade.

To upgrade the IMPAX 6.2 or later database data and schema to IMPAX 6.5.1

1. Log into the Database Server as the **oracle** user.

   Important!

   For Oracle Data Guard servers, upgrade the database data and schema only on the primary Database Server.

2. Start the listener by typing

   lsnrctl start

3. Change to the **/usr/mvf-mig6/bin** directory.
4. If upgrading from IMPAX 6.5, type

./database-upgrade-script

Otherwise, type

./database-upgrade-script -v {**62** | **63** | **64**}

For example, to upgrade an IMPAX 6.2 system to 6.5.1, type **./database-upgrade-script -v 62**. To upgrade an IMPAX 6.3 system to 6.5.1, type **./database-upgrade-script -v 63**.

The following prompt appears:

```
Ready to upgrade database from current system version version_number.
Do you want to proceed [q to quit]?
```

5. Verify that the *version_number* returned is correct—for example, that it says **62** if upgrading from IMPAX 6.2. If so, press **Enter** to continue.

   If the version is not correct, type **q** and press **Enter**, then repeat step 4 with the correct version number specified.

6. When prompted for a report source, in most cases, type **UNKNOWN**. If using a queryable RIS and multiple Connectivity Managers, type the value used for the Connectivity Manager **issuer_of_*** and **mcf_bls_report_workflow domain_id** fields.

   This value is the facility sending name entered in the HL7 In field in the Connectivity Manager Service Tools when mapping report sources.

7. Respond appropriately to other prompts that appear.

The database is upgraded.

Important!

The following procedure applies only to Oracle Data Guard servers.

To complete the upgrade of the Oracle Data Guard Database Servers to IMPAX 6.5.1

1. Log into both the primary and standby IMPAX 6.5.1 Database Servers as the **root** user.
2. In the **/var/opt/oracle** directory, rename the following files:
   - From `listener.ora` to **listener.ora.new**
   - From `tnsnames.ora` to `tnsnames.ora.new`
   - From `listener.ora.dg`*xx* to **listener.ora**, where *xx* is the IMPAX version; for example, *65*
   - From `tnsnames.ora.dg`*xx* to **tnsnames.ora**, where *xx* is the IMPAX version; for example, *65*
3. On the primary Database Server, as the **oracle** user, start the public listener; type

   lsnrctl start listener_public
4. After a few seconds, to list both the private and public listener processes, type

   psg tns

6. Checking the upgrade status

(Topic number: 10196)

After upgrading the database, check the log file to ensure that the upgrade was successful.

Important!

We recommend checking the migration log file after each leg of an upgrade before moving onto the next leg.

To check the upgrade status

1. On the Database Server, log in as the oracle user and open the log file **/usr/mvf-mig6/data/logs/migrate_database_to6.5.log**.

   If the following message appears in the log file, disregard it.

   ```
   E 2010.03.14 11:53:25.972(1)/mig6-database-upgrade table_add:add_sind_default:
   Column PATIENT_ID is indexed, no action is taken.
   ```

2. Ensure that `Migration Complete Successful` appears at the end of the log file.
3. If this message does not appear, something went wrong with the upgrade.
   a. Review the rest of the log file to see where the upgrade failed.
   b. Solve the problem.
   c. Rerun the upgrade script.

7. Upgrading the Oracle Data Guard package

(Topic number: 67662)

Important!

This topic applies only to servers running Oracle Data Guard.

To use Oracle Data Guard, the existing IMPAXoradg package must be removed after an upgrade and replaced with the new version.

For information about configuring Oracle Data Guard, see *Configuring Oracle Data Guard* (refer to page 143).

To upgrade the Oracle Data Guard package

1. Log into the primary Database Server as the **root** user.
2. Change to the IMPAX software repository directory.

3. To remove the existing package, type **pkgrm IMPAXoradg**.
4. Change to the **IMPAX_R6.5.1-build_number** directory.
5. Type **pkgadd -d . IMPAXoradg**.
6. To verify that the upgraded package was installed, type **pkginfo -l IMPAXoradg**.
7. Repeat all previous steps on the standby Database Server.

Upgrading Solaris 10 AS3000 components to IMPAX 6.5.1

4

Important!

If upgrading IMPAX servers on Solaris 9, perform the *Upgrading Solaris 9 AS3000 components to IMPAX 6.5.1* (refer to page 57) tasks instead.

If upgrading IMPAX servers on Solaris 10, run the cluster upgrade process to upgrade the Database Server, AS3000 (Solaris) Network Gateways, and AS3000 (Solaris) Archive Servers to IMPAX 6.5.1. This applies to both single-host and dedicated Database Server configurations.

If you are replacing the existing Database Server with a new server, first back up the database files. After installing the IMPAX 6.5.1 server software on the new server, copy the backed-up database files from the previous release of IMPAX onto the new server (refer to page 62).

1. Installing Solaris 10 patches

(Topic number: 58098)

To download and install Solaris 10 patches, you need a Solaris maintenance agreement and login details, which you can obtain from Oracle.

You must install the Solaris 10 patches recommended by Oracle on all IMPAX servers running Solaris 10.

To install Solaris 10 patches

1. Log into the Solaris support website using your maintenance agreement credentials.
2. Under Patches and Updates, select the **Solaris 10** patch set.

3. Review the Readme file associated with this patch set and make note of the password which is needed to run the installation script.

   Note:

   The latest, most complete patch installation information, including the password needed to run the installation script, is included in the Readme file provided. You must review it.

4. Download the patch file to a directory of your choice, such as the /agfa directory.

   The patch file is called 10_Recommended.zip.

5. Log in as root and change to the directory containing the patch file. (Mount the location, if necessary.)
6. Unzip the patches. Type

   unzip -q 10_Recommended.zip

7. Delete the 10_Recommended.zip file. Type

   rm 10_Recommended.zip

8. Change to the **10_Recommended/** directory.
9. Switch to single-user mode by typing **init s** and providing the root password.

   Important!

   Do not skip this step; doing so can create problems in Solaris.

10. Run the patch installation script. Type

    ./installcluster *password*

    where *password* is the password provided in the Readme file.

11. When the process is complete, reboot the server. Type

    shutdown -y -i6 -g0

12. When the server is restarted, in a browser, go to the Solaris support website again.
13. Under Patches and Updates, select the **J2SE Solaris 10** patch set.
14. Review the Readme file associated with this patch set.
15. Download the patch file to the same directory as the previous patch.

    The patch file is called J2SE_Solaris_10_Recommended.zip.

16. Change to the directory containing the patch file. (Mount the location, if necessary.)
17. Unzip the patches. Type

    unzip -q J2SE_Solaris_10_Recommended.zip

18. To delete the J2SE_Solaris_10_Recommended.zip file, type

    rm J2SE_Solaris_10_Recommended.zip

19. Change to the **J2SE_Solaris_10_Recommended/** directory.
20. Switch to system administrator mode by typing **init s** and providing the root password.
21. Execute the patch installation script. Type

    ./install_cluster
22. When the patch installation is complete, reboot the server. Type

    shutdown -y -i6 -g0

All the patches needed for IMPAX 6.5.1 are now installed.

2. Upgrading a Solaris server to Oracle Client 10.2.0.4.0

(Topic number: 10162)

In a multi-host configuration, you must upgrade the Oracle Client software to version 10.2.0.4.0. Perform this task on all AS3000 Network Gateway and Archive Server machines to be upgraded.

The upgrade-oracle script upgrades Oracle Client to Oracle 10.2.0.4.0 from versions 9.2.0.4, 10.1.0.2, 10.2.0.2.0, or 10.2.0.3.0.

You can upgrade Oracle either from the Oracle for Solaris DVD or a software repository.

To upgrade a Solaris server to Oracle Client 10.2.0.4.0

1. On the server running the Oracle Client, log in as root user and change to the **/usr/mvf-mig6/bin** directory.
2. Type **./upgrade-oracle**
3. When prompted, type the path to the Oracle 10.2.0.4.0 software repository.

   For example, ***/software_repository_path***
4. If the following error message appears:

   ```
   Unable to stop the cron process. Stop it manually as user root in /etc/init.d
   and execute ./cron stop before re-running this script.
   ```

   Manually disable the cron process. As the **root** user, type

   svcadm disable svc:/system/cron:default

   Note:

   Re-enable cron after the upgrade has completed. Type **svcadm enable svc:/system/cron:default**.

The upgrade takes approximately 30 minutes to complete. You can ignore the following warnings:

```
chmod: WARNING: can't access /usr/oracle/current/lib/ libagtsh.so
chmod: WARNING: can't access /usr/oracle/current/lib32/ libagtsh.so
```

3. Verifying that Solaris patches are installed

(Topic number: 60379)

Since Solaris patches have already been installed, confirm that the Sun_rec_patches_installed file (it is a hidden file) exists in the /root partition of all the Solaris servers. When the IMPAX application is being upgraded, the program checks for the existence of this file. If this file is not found, the script requires the user to install the Solaris patches again.

To verify that Solaris patches are installed

1. Log in as the **root** user.
2. Change to the root directory.
3. Type

   showrev -p
4. Check whether the Sun_rec_patches_installed file exists.
5. If the file does not exist, type the following command:

   touch .Sun_rec_patches_installed

4. Running the Trust Tool and cluster upgrade

(Topic number: 47687)

Note:

If, for some reason, the Trust Tool cannot be run or you do not want to upgrade the cluster as a whole, upgrade the Solaris servers individually by running the impax_install script (refer to page 171).

If you are replacing existing AS3000 Solaris servers with new servers, the following procedure does not apply and you can skip ahead to *Copying the backed-up database files to a new or restaged IMPAX 6.5.1 server* (refer to page 62).

Procedures for upgrading Windows servers in the cluster (refer to page 90) are provided later in this guide.

Before starting the cluster upgrade, perform the following prerequisite tasks:

1. Confirm that your upgrade path is supported. Only specific paths are supported, and it may not be possible to upgrade certain versions and/or SUs. For further details, see *Valid IMPAX upgrade paths* (refer to page 9).
2. Open the /install_info file and check the REPOSITORY path.
3. If the REPOSITORY path is /cdrom/cdrom0 and you are upgrading IMPAX using DVD, then the path need not be changed. But if you are upgrading from a software repository

(recommended) and this path is not listed, change the REPOSITORY path appropriately, using a text editor such as 'vi'.

4. If using Oracle Data Guard, remove any unnecessary IMPAX package entries from the /install_info file. These entries may be left over from the previous installation of the primary and standby Database Servers; for example, `IMAGE_CACHE='y'`.

   Important!

   Oracle Data Guard Database Servers should be dedicated Database Servers without any Network Gateway, Archive Server, or cache components installed.

5. Save and close the /install_info file.
6. Back up the /etc/system file in case problems occur during migration.

When upgrading AS3000 Database Server, Network Gateway, and Archive Server stations to IMPAX 6.5.1, use the Trust Tool as described here to establish a bidirectional SSH trust relationship with all Solaris servers, allowing for remote login and file copying in a single step. This cluster upgrade procedure also works for AS3000 single-host configurations.

To run the Trust Tool and cluster upgrade

1. On the Solaris 10 server hosting the repository:
   a. Log in as user **root**.
   b. Modify the /etc/ssh/sshd_config file by setting the parameter PermitRootLogin to **yes**.
   c. To restart the ssh daemon, type **svcadm restart ssh**.
2. On the repository machine, log in as user **root**.
3. Change to the ***software_repository_path*** directory.

   If upgrading from the DVD, the *software_repository_path* is **/cdrom/cdrom0**.
4. Type

   ./trust_tool
5. Select option **a - Build File /var/tmp/mvftrust/hosts.cluster**.

   This creates the file /var/tmp/mvftrust/hosts.cluster, containing a list of the host names of the servers to be upgraded.
6. Select option **q - Quit**.
7. In a text editor such as vi, edit the /var/tmp/mvftrust/hosts.cluster file and remove the names of any non-AS3000 server from the file (for example, names of Application Servers, AS300 Network Gateways, and so on).
8. Change to the ***software_repository_path***.
9. Type

   ./trust_tool
10. Select option **b - Establish Trust Relation with Target Hosts**.

    This step establishes trust between the software repository server and the servers to be upgraded.

11. Provide the passwords (for the root user) requested by the script.

    Should the `unable to initialize mechanism library` message appear, you can ignore.

12. If you receive the error message `WARNING: POSSIBLE DNS SPOOFING DETECTED!` with several lines of text and `FAILED to generate keys on host: <host_name>` at the end:

    Note that each line must start with *host_name* and *IP_address*. One line may wrap to two or more lines so you must be careful when editing.

    a. Make a backup copy of the /.ssh/known_hosts file.

    b. Open the /.ssh/known_hosts file in a vi or other text editor, go to the beginning of the line containing the *host_name* specified in the error message, delete the offending line, and save the file.

    c. Run **./trust_tool** and select option **b** again.

    Note:

    If you have not added the PermitRootLogin to the /etc/ssh/sshd_config file and then attempt to establish a trust relationship with the hosts, another error may occur. Remove the forgotten hosts from the /.ssh/known_hosts file, edit the PermitRootLogin, then reestablish the trust relationship.

13. Change to the ***software_repository_path***.

14. Type

    ./trust_tool

15. Select option **c - Check Trust Relation with Target Hosts**.

    If you omit this step, you may receive a large number of prompts for passwords when you run the cluster_install upgrade process later in this process.

16. Copy the file **/var/tmp/mvftrust/hosts.cluster** to **/hosts.cluster**.

17. Ensure that the name of the software repository machine is on the list. If it is not, add it and save the file.

18. If you are logged in as the **oracle** user on any machines in the cluster (the machines are listed in the hosts.cluster file), log out now.

    Important!

    You must complete this step; the upgrade will not run if you are logged in as the **oracle** user on any machines in the cluster.

19. Change to the ***software_repository_path***.

20. Type

    ./cluster_install upgrade

21. At the prompt:

    ```
    Is it OK to shutdown the entire cluster at this time? [yes,no,?,q]
    ```

type **yes**.

The cluster is shut down and the AS3000 software upgraded.

22. At the prompt:

    `Is it OK to start up the entire cluster at this time? [yes,no,?,q]`

    type **yes**.

23. For security, disallow the remote login as **root** on the repository machine and targets. On the repository machine and on each Solaris target machine:
    a. Log in as user **root**.
    b. Modify the /etc/ssh/sshd_config file by setting the parameter PermitRootLogin to **no**.
    c. To restart the ssh daemon, type **svcadm restart ssh**.

5. Testing the AS3000 Database Server upgrade

(Topic number: 60533)

After upgrading the AS3000 Database Server, we recommend performing a quick test to ensure that the upgrade was successful.

To test the AS3000 Database Server upgrade

1. Log into the Database Server as the **oracle** or **service** user.
2. Change to the **/usr/mvf/bin** directory.
3. Type

   ldd mvf-* | grep -i "file not found"
4. Confirm that error messages such as `File not found` do not appear.

   If any of the libraries are missing, contact Agfa support for emergency recovery processes.
5. Verify that CLUI works.

Upgrading Solaris 9 AS3000 components to IMPAX 6.5.1

5

Important!

If upgrading existing IMPAX servers on Solaris 10, perform the *Upgrading Solaris 10 AS3000 components to IMPAX 6.5.1* (refer to page 50) tasks previously described instead.

To complete the upgrade of IMPAX AS3000 stations on Solaris 9, including the Database Server and any Archive Servers or Network Gateways, the servers must be restaged with Solaris 10 and IMPAX 6.5.1.

Before the servers are restaged, the Database Server is shut down again and another cold backup of the database is performed.

After the restaging, the backup of the Oracle database is restored on the newly staged Database Server.

Note:

For Oracle Data Guard Database Servers, both the primary and standby servers must be restaged and have their backups restored.

1. Shutting down the Database Server

(Topic number: 10156)

Run these commands on the Database Server before upgrading the software or restaging the server.

To shut down the Database Server

1. Log into the Database Server as the **mvf** user.

or

When restaging a Database Server already running Oracle 10.2.0.4.2, log in as the **oracle** user.

2. To shut down the database, type

   dbshutmvf

3. To shut down the listener, type

   lsnrctl stop

4. To confirm that all IMPAX and Oracle processes have stopped, type

   psg mvf

   psg ora

   psg tns

5. Verify that, in each of these cases, nothing is returned.

2. Storing a cold backup of the database and other Oracle configuration files

(Topic number: 59281)

Back up the Oracle data and configuration files immediately before the start of the upgrade or restage. This procedure can take a significant amount of time. To estimate how long it will be, check the duration of warm backups as recorded in the /data/logs/backup.log file.

To store a cold backup of the database and other Oracle configuration files

1. If using a NFS share to store the backup, start the NFS service on the server where the backup files will be stored.

   On Solaris 10, type

   su -

   svcadm -v enable -r network/nfs/server

   or

   On Solaris 9, type

   su -

   cd /etc/rc3.d

   ./s15nfs.server start

2. To share the directory that the IMPAX server will be writing to use a Unix text editor such as vi. For example, type

   su -

   vi /etc/dfs/dfstab

3. Add the following line

share -F nfs -o rw,anon=0 ***path_to_backup_location_directory***

4. Save and close the file.
5. On the IMPAX server, mount the share as the **root** user. For example, type

   mkdir /*backup_location*

   mount -o rw,bg,hard,rsize=32768,wsize=32768,vers=3,forcedirectio,nointr,suid ***server_containing_backup*:*absolute_path_to_backup_location_directory* /*backup_location***
6. As the **root** user, copy the appropriate files to the backup location.

Original directory	File	IMPAX 6.5.1 directory	Description
/dbase	all files under this directory	/dbase	Oracle data files and control files
/usr/oracle/current/dbs or /opt/oracle/current/dbs (if replacing an IMPAX 6.4 or later server)	orapw	/opt/oracle/current/dbs	Oracle password file location
	initMVF.ora		Oracle text initialization parameter file
	spfileMVF.ora		Oracle binary initialization parameter file (only if running Oracle 10.2)
	dr1MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
	dr2MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
/var/opt/oracle	tnsnames.ora	/var/opt/oracle	Oracle Naming Configuration
	listener.ora		Oracle Listener Configuration
	sqlnet.ora		Oracle SQLNET Configuration

Original directory	File	IMPAX 6.5.1 directory	Description
	listener.ora.dg*xx*		IMPAX 6.4 or later Oracle Listener Configuration backup
	tnsnames.ora.dg*xx*		IMPAX 6.4 or later Oracle Naming Configuration backup
	tnsnames.ora.client		Oracle Listener Configuration for clients (only when Oracle Data Guard is configured)
/cache/mvfcache	all files under this directory	/cache/mvf/cache	IMPAX cache—only if the cache directory is physically on the Database Server
/usr/mvf	dg_info	/usr/mvf	Oracle Data Guard cluster information for IMPAX

For example:

cp -r /dbase /*backup_location*

cp -r /usr/oracle/current/dbs/orapw /*backup_location*

cp -r /usr/oracle/current/dbs/initMVF.ora /*backup_location*

cp -r /usr/oracle/current/dbs/spfileMVF.ora /*backup_location*

cp -r /usr/oracle/current/dbs/dr1MVF.dat /*backup_location*

cp -r /usr/oracle/current/dbs/dr2MVF.dat /*backup_location*

cp -r /var/opt/oracle/tnsnames.ora /*backup_location*

cp -r /var/opt/oracle/listener.ora /*backup_location*

cp -r /var/opt/oracle/sqlnet.ora /*backup_location*

cp -r /var/opt/oracle/listener.ora.dg*xx* /*backup_location* where *xx* is the IMPAX version

cp -r /var/opt/oracle/tnsnames.ora.dg*xx* /*backup_location* where *xx* is the IMPAX version

cp -r /var/opt/oracle/tnsnames.ora.client /*backup_location*

cp -r /usr/mvf/dg_info /*backup_location*

cp -r /cache/mvfcache /*backup_location*

3. Completing the restaging of the AS3000 stations

(Topic number: 67230)

Important!

This topic applies when upgrading IMPAX stations on Solaris 9 to IMPAX 6.5.1 or restaging existing Solaris 10 servers.

To set up Solaris 10 servers and install and configure IMPAX 6.5.1 on the servers, refer to the instructions in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*, specifically the "Setting up a Solaris server", "Creating the Database Server", "Creating the Network Gateway", and "Creating the Archive Server" sections.

To complete the restaging of the AS3000 stations

1. Install and configure the Database Server, restaging it with Solaris 10 and IMPAX 6.5.1.

   Important!

   For Oracle Data Guard Database Servers, both the primary and standby servers must be restaged. Ensure that the directory location for the Flashback area matches that of the old server.

2. Install and configure any other AS3000 servers, such as Archive Servers or Network Gateways.
3. Shut down the Database Server again, stopping all IMPAX and Oracle processes.
4. Restore the database (refer to page 62) by copying all the database files from the previous cold backup to the newly staged Database Server. (For Oracle Data Guard Database Servers, restore the backups on both the primary and the standby servers.)
5. Check and restart the database after restaging (refer to page 65).

   or

   Check and restart the Oracle Data Guard servers (refer to page 66).

4. Copying the backed-up database files to a new or restaged IMPAX 6.5.1 server

(Topic number: 6892)

Important!

This topic applies only if you are replacing the existing server with a new server, or are restaging the existing server.

When replacing the existing server with a new server, or restaging the existing server, first back up the database files (refer to page 58). After installing the IMPAX 6.5.1 server software on the new (or restaged) servers, copy the backed-up database files from the previous release of IMPAX to the new servers, as described in this topic.

CAUTION!

Be very careful not to delete any live database files. Only perform this procedure on a new or restaged Database Server that has not had any clinical use, even as a training server. Do not perform this procedure on *any* production, training, or traveling servers. When files are being copied, take care to preserve file and directory ownership and permissions.

To copy the backed-up database files to a new or restaged IMPAX 6.5.1 server

1. On the new IMPAX 6.5.1 Database Server, stop all IMPAX processes. As the **root** user, type

   stop_impax

2. Stop all Oracle processes. As the **mvf** user or **oracle** user (if running IMPAX 6.4 or later), type

   lsnrctl stop listener

   lsnrctl stop listener_public (for Oracle Data Guard server)

   dbshutmvf

   Note:

   For Oracle Data Guard servers, stop Oracle processes on both the primary and standby servers.

3. Log in as **root** and change to the **/dbase** directory.
4. To remove all the database files in the directory, type

   rm -f data1/*

5. Repeat the previous step for any subdirectories. Be sure to delete only the files—leave the directory structure intact.

6. Restore every file from the backup location. If a backup is stored on a NFS share, first mount the share. As the **root** user, type

   mount -o rw,bg,hard,rsize=32768,wsize=32768,vers=3,forcedirectio,nointr,suid *server_containing_backup*:*absolute_path_to_backup_location_directory* /*backup_location*

   Restore the following files to the indicated IMPAX 6.5.1 directory.

Original directory	File	IMPAX 6.5.1 directory	Description
/dbase	all files under this directory	/dbase	Oracle data files and control files
/usr/oracle/current/dbs or /opt/oracle/current/dbs (if replacing an IMPAX 6.4 or later server)	orapw	/opt/oracle/current/dbs	Oracle password file location
	initMVF.ora		Oracle text initialization parameter file
	spfileMVF.ora		Oracle binary initialization parameter file (only if running Oracle 10.2)
	dr1MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
	dr2MVF.dat		Oracle Data Guard configuration file (only when Oracle Data Guard is configured)
/var/opt/oracle	tnsnames.ora	/var/opt/oracle	Oracle Naming Configuration
	listener.ora		Oracle Listener Configuration
	sqlnet.ora		Oracle SQLNET Configuration
	listener.ora.dg*xx*		IMPAX 6.4 or later Oracle Listener Configuration backup

Original directory	File	IMPAX 6.5.1 directory	Description
	tnsnames.ora.dg*xx*		IMPAX 6.4 or later Oracle Naming Configuration backup
	tnsnames.ora.client		Oracle Listener Configuration for clients (only when Oracle Data Guard is configured)
/cache/mvfcache	all files under this directory	/cache/mvf/cache	IMPAX cache—only if the cache directory is physically on the Database Server
/usr/mvf	dg_info	/usr/mvf	Oracle Data Guard cluster information for IMPAX

For example:

cp -r /*backup_location*/dbase/* /dbase

cp -r /*backup_location*/orapw /opt/oracle/current/dbs

cp -r /*backup_location*/initMVF.ora /opt/oracle/current/dbs

cp -r /*backup_location*/spfileMVF.ora /opt/oracle/current/dbs

cp -r /*backup_location*/dr1MVF.ora /opt/oracle/current/dbs

cp -r /*backup_location*/dr2MVF.ora /opt/oracle/current/dbs

cp -r /*backup_location*/tnsnames.ora /var/opt/oracle

cp -r /*backup_location*/listener.ora /var/opt/oracle

cp -r /*backup_location*/sqlnet.ora /var/opt/oracle

cp -r /*backup_location*/tnsnames.ora.dg*xx* /var/opt/oracle where *xx* is the IMPAX version

cp -r /*backup_location*/listener.ora.dg*xx* /var/opt/oracle where *xx* is the IMPAX version

cp -r /*backup_location*/listener.ora.client /var/opt/oracle

cp -r /*backup_location*/dg_info /usr/mvf

cp -r /*backup_location*/mvfcache /cache

7. Ensure that all copied files are owned by the oracle user, with the exception of the cache directory, which must be owned by mvf:mitra. To change the ownership, log in as the **root** user, and type

   chown -R oracle:dba *file_or_directory_name*

   For example:

   chown -R oracle:dba /dbase

   chown -R oracle:dba /opt/oracle/current/dbs/orapw

   chown -R oracle:dba /opt/oracle/current/dbs/initMVF.ora

chown -R oracle:dba /opt/oracle/current/dbs/spfileMVF.ora

chown -R oracle:dba /opt/oracle/current/dbs/dr1MVF.ora

chown -R oracle:dba /opt/oracle/current/dbs/dr2MVF.ora

chown -R oracle:dba /var/opt/oracle/tnsnames.ora

chown -R oracle:dba /var/opt/oracle/listener.ora

chown -R oracle:dba /var/opt/oracle/tnsnames.ora.dg*xx* where *xx* is the IMPAX version

chown -R oracle:dba /var/opt/oracle/listener.ora.dg*xx* where *xx* is the IMPAX version

chown -R oracle:dba /var/opt/oracle/tnsnames.ora.client

chown -R oracle:dba /var/opt/oracle/sqlnet.ora

chown -R oracle:dba /usr/mvf/dg_info

5. Checking and restarting the database after restaging

(Topic number: 68248)

Important!

This topic applies when a server has been staged or restaged with IMPAX 6.5.1 on Solaris 10.

Make sure that you have already restored the database (refer to page 62) by copying all the database files from the previous cold backup to the newly staged Database Server.

If checking and restarting an Oracle Data Guard database, skip these instructions and proceed with *Checking and restarting the database after restaging, for Oracle Data Guard* (refer to page 66).

To check and restart the database after restaging

1. Confirm that all restored files have *oracle:dba* ownership.
2. Start the database and confirm that no errors appear.
3. Reboot the Database Server.

6. Checking and restarting the database after restaging, for Oracle Data Guard

(Topic number: 113612)

Important!

This topic applies when a Oracle Data Guard server has been staged or restaged with IMPAX 6.5.1 on Solaris 10.

Make sure that you have already restored the database (refer to page 62) by copying all the database files from the previous cold backup to the newly staged Database Server.

To check and restart the database after restaging, for Oracle Data Guard

1. Start up Oracle on both the primary and standby Database Servers.
   a. As the **oracle** user, type **sqlplus as / sysdba**
   b. At the sql prompt, type **startup mount**
   c. Confirm that there are no errors on the console.
2. Start the listener on both Database Servers.
   a. On the primary server, as the **oracle** user, type

      lsnrctl start listener

      lsnrctl start listener_public
   b. On the standby server, as the **oracle** user, type

      lsnrctl start listener
   c. After a few seconds, to list both the private and public listener processes, type

      psg tns
3. Check the Data Guard configuration.
   a. On the primary server, as the **oracle** user, type

      dgmgrl sys/stayout@mvf1
   b. At the DGMGRL prompt, type

      show configuration
   c. Confirm that SUCCESS is reported.
   d. To quit, type **exit**.
4. Confirm that there are no problems with the standby archive logs. On the primary server, as the **oracle** user, type

   check_standby

5. Confirm that clui can connect to the database. On the primary server, as the **oracle** user, type **clui**
6. To exit clui, type **exit**.
7. Reboot both the primary and standby Database Servers.
8. After the servers have rebooted, start the public listener on the primary server.

Upgrading an IMPAX 6.5 AS3000 cluster to IMPAX 6.5.1

6

These tasks apply only when upgrading an AS3000 cluster already on IMPAX 6.5.

1. Upgrading the IMPAX 6.2 or later database data and schema to IMPAX 6.5.1

(Topic number: 60408)

Important!

Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

Upgrading the 6.2 or later database schema to 6.5.1 requires the IMPAX Migration Tools. For Migration Tools installation instructions, refer to the "Installing the IMPAX 6.5.1 Migration Toolbox" section in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 6.2 or later to IMPAX 6.5.1*.

During the schema upgrade, a MAP_EVENT_AUDIT.dmp file is created in the /usr/mvf-mig6/data directory. Ensure that enough space is available for this file: upwards of 10 GB, depending on the size of the database and the MAP_AUDIT_EVENT table.

CAUTION!

Any customization to the database—such as extra indexes, stored procedures, or triggers—may affect the schema upgrade. We recommend removing such customizations prior to the upgrade.

To upgrade the IMPAX 6.2 or later database data and schema to IMPAX 6.5.1

1. Log into the Database Server as the **oracle** user.

   Important!

   For Oracle Data Guard servers, upgrade the database data and schema only on the primary Database Server.

2. Start the listener by typing

   lsnrctl start

3. Change to the **/usr/mvf-mig6/bin** directory.
4. If upgrading from IMPAX 6.5, type

   ./database-upgrade-script

   Otherwise, type

   ./database-upgrade-script -v {**62** | **63** | **64**}

   For example, to upgrade an IMPAX 6.2 system to 6.5.1, type **./database-upgrade-script -v 62**. To upgrade an IMPAX 6.3 system to 6.5.1, type **./database-upgrade-script -v 63**.

   The following prompt appears:

   ```
   Ready to upgrade database from current system version version_number.
   Do you want to proceed [q to quit]?
   ```

5. Verify that the *version_number* returned is correct—for example, that it says **62** if upgrading from IMPAX 6.2. If so, press **Enter** to continue.

   If the version is not correct, type **q** and press **Enter**, then repeat step 4 with the correct version number specified.

6. When prompted for a report source, in most cases, type **UNKNOWN**. If using a queryable RIS and multiple Connectivity Managers, type the value used for the Connectivity Manager **issuer_of_*** and **mcf_bls_report_workflow domain_id** fields.

   This value is the facility sending name entered in the HL7 In field in the Connectivity Manager Service Tools when mapping report sources.

7. Respond appropriately to other prompts that appear.

The database is upgraded.

Important!

The following procedure applies only to Oracle Data Guard servers.

To complete the upgrade of the Oracle Data Guard Database Servers to IMPAX 6.5.1

1. Log into both the primary and standby IMPAX 6.5.1 Database Servers as the **root** user.
2. In the **/var/opt/oracle** directory, rename the following files:
   - From `listener.ora` to **listener.ora.new**

- From `tnsnames.ora` to `tnsnames.ora.new`
- From `listener.ora.dg`*xx* to **listener.ora**, where *xx* is the IMPAX version; for example, *65*
- From `tnsnames.ora.dg`*xx* to **tnsnames.ora**, where *xx* is the IMPAX version; for example, *65*

3. On the primary Database Server, as the **oracle** user, start the public listener; type

   lsnrctl start listener_public
4. After a few seconds, to list both the private and public listener processes, type

   psg tns

2. Checking the upgrade status

(Topic number: 10196)

After upgrading the database, check the log file to ensure that the upgrade was successful.

Important!

We recommend checking the migration log file after each leg of an upgrade before moving onto the next leg.

To check the upgrade status

1. On the Database Server, log in as the oracle user and open the log file **/usr/mvf-mig6/data/logs/migrate_database_to6.5.log**.

   If the following message appears in the log file, disregard it.

   ```
   E 2010.03.14 11:53:25.972(1)/mig6-database-upgrade table_add:add_sind_default:
   Column PATIENT_ID is indexed, no action is taken.
   ```
2. Ensure that `Migration Complete Successful` appears at the end of the log file.
3. If this message does not appear, something went wrong with the upgrade.
   a. Review the rest of the log file to see where the upgrade failed.
   b. Solve the problem.
   c. Rerun the upgrade script.

3. Upgrading the Oracle Data Guard package

(Topic number: 67662)

Important!

This topic applies only to servers running Oracle Data Guard.

To use Oracle Data Guard, the existing IMPAXoradg package must be removed after an upgrade and replaced with the new version.

For information about configuring Oracle Data Guard, see *Configuring Oracle Data Guard* (refer to page 143).

To upgrade the Oracle Data Guard package

1. Log into the primary Database Server as the **root** user.
2. Change to the IMPAX software repository directory.
3. To remove the existing package, type **pkgrm IMPAXoradg**.
4. Change to the **IMPAX_R6.5.1-build_number** directory.
5. Type **pkgadd -d . IMPAXoradg**.
6. To verify that the upgraded package was installed, type **pkginfo -l IMPAXoradg**.
7. Repeat all previous steps on the standby Database Server.

4. Running the Trust Tool and cluster upgrade

(Topic number: 47687)

Note:

If, for some reason, the Trust Tool cannot be run or you do not want to upgrade the cluster as a whole, upgrade the Solaris servers individually by running the impax_install script (refer to page 171).

If you are replacing existing AS3000 Solaris servers with new servers, the following procedure does not apply and you can skip ahead to *Copying the backed-up database files to a new or restaged IMPAX 6.5.1 server* (refer to page 62).

Procedures for upgrading Windows servers in the cluster (refer to page 90) are provided later in this guide.

Before starting the cluster upgrade, perform the following prerequisite tasks:

1. Confirm that your upgrade path is supported. Only specific paths are supported, and it may not be possible to upgrade certain versions and/or SUs. For further details, see *Valid IMPAX upgrade paths* (refer to page 9).
2. Open the /install_info file and check the REPOSITORY path.
3. If the REPOSITORY path is /cdrom/cdrom0 and you are upgrading IMPAX using DVD, then the path need not be changed. But if you are upgrading from a software repository (recommended) and this path is not listed, change the REPOSITORY path appropriately, using a text editor such as 'vi'.
4. If using Oracle Data Guard, remove any unnecessary IMPAX package entries from the /install_info file. These entries may be left over from the previous installation of the primary and standby Database Servers; for example, `IMAGE_CACHE='y'`.

   Important!

   Oracle Data Guard Database Servers should be dedicated Database Servers without any Network Gateway, Archive Server, or cache components installed.

5. Save and close the /install_info file.
6. Back up the /etc/system file in case problems occur during migration.

When upgrading AS3000 Database Server, Network Gateway, and Archive Server stations to IMPAX 6.5.1, use the Trust Tool as described here to establish a bidirectional SSH trust relationship with all Solaris servers, allowing for remote login and file copying in a single step. This cluster upgrade procedure also works for AS3000 single-host configurations.

To run the Trust Tool and cluster upgrade

1. On the Solaris 10 server hosting the repository:
   a. Log in as user **root**.
   b. Modify the /etc/ssh/sshd_config file by setting the parameter PermitRootLogin to **yes**.
   c. To restart the ssh daemon, type **svcadm restart ssh**.
2. On the repository machine, log in as user **root**.
3. Change to the ***software_repository_path*** directory.

   If upgrading from the DVD, the *software_repository_path* is **/cdrom/cdrom0**.
4. Type

   ./trust_tool
5. Select option **a - Build File /var/tmp/mvftrust/hosts.cluster**.

   This creates the file /var/tmp/mvftrust/hosts.cluster, containing a list of the host names of the servers to be upgraded.
6. Select option **q - Quit**.
7. In a text editor such as vi, edit the /var/tmp/mvftrust/hosts.cluster file and remove the names of any non-AS3000 server from the file (for example, names of Application Servers, AS300 Network Gateways, and so on).

8. Change to the ***software_repository_path***.
9. Type

   ./trust_tool
10. Select option **b - Establish Trust Relation with Target Hosts**.

    This step establishes trust between the software repository server and the servers to be upgraded.
11. Provide the passwords (for the root user) requested by the script.

    Should the `unable to initialize mechanism library` message appear, you can ignore.
12. If you receive the error message `WARNING: POSSIBLE DNS SPOOFING DETECTED!` with several lines of text and `FAILED to generate keys on host: <host_name>` at the end:

    Note that each line must start with *host_name* and *IP_address*. One line may wrap to two or more lines so you must be careful when editing.

    a. Make a backup copy of the /.ssh/known_hosts file.

    b. Open the /.ssh/known_hosts file in a vi or other text editor, go to the beginning of the line containing the *host_name* specified in the error message, delete the offending line, and save the file.

    c. Run **./trust_tool** and select option **b** again.

    Note:

    If you have not added the PermitRootLogin to the /etc/ssh/sshd_config file and then attempt to establish a trust relationship with the hosts, another error may occur. Remove the forgotten hosts from the /.ssh/known_hosts file, edit the PermitRootLogin, then reestablish the trust relationship.
13. Change to the ***software_repository_path***.
14. Type

    ./trust_tool
15. Select option **c - Check Trust Relation with Target Hosts**.

    If you omit this step, you may receive a large number of prompts for passwords when you run the cluster_install upgrade process later in this process.
16. Copy the file **/var/tmp/mvftrust/hosts.cluster** to **/hosts.cluster**.
17. Ensure that the name of the software repository machine is on the list. If it is not, add it and save the file.
18. If you are logged in as the **oracle** user on any machines in the cluster (the machines are listed in the hosts.cluster file), log out now.

    Important!

    You must complete this step; the upgrade will not run if you are logged in as the **oracle** user on any machines in the cluster.

19. Change to the ***software_repository_path***.
20. Type

    ./cluster_install upgrade
21. At the prompt:

    `Is it OK to shutdown the entire cluster at this time? [yes,no,?,q]`

    type **yes**.

    The cluster is shut down and the AS3000 software upgraded.
22. At the prompt:

    `Is it OK to start up the entire cluster at this time? [yes,no,?,q]`

    type **yes**.
23. For security, disallow the remote login as **root** on the repository machine and targets. On the repository machine and on each Solaris target machine:
    a. Log in as user **root**.
    b. Modify the /etc/ssh/sshd_config file by setting the parameter PermitRootLogin to **no**.
    c. To restart the ssh daemon, type **svcadm restart ssh**.

5. Testing the AS3000 Database Server upgrade

(Topic number: 60533)

After upgrading the AS3000 Database Server, we recommend performing a quick test to ensure that the upgrade was successful.

To test the AS3000 Database Server upgrade

1. Log into the Database Server as the **oracle** or **service** user.
2. Change to the **/usr/mvf/bin** directory.
3. Type

   ldd mvf-* | grep -i "file not found"
4. Confirm that error messages such as `File not found` do not appear.

   If any of the libraries are missing, contact Agfa support for emergency recovery processes.
5. Verify that CLUI works.

Completing the upgrade of Solaris components to IMPAX 6.5.1

7

Some additional tasks must be performed to complete the upgrade of the IMPAX servers on Solaris to IMPAX 6.5.1.

1. Updating odbc.ini after upgrading an AS3000 Network Gateway or Archive Server

(Topic number: 110722)

After upgrading an Oracle Data Guard cluster, update the odbc.ini file on any AS3000 Network Gateway or Archive Server station.

Important!

This update applies only after upgrading an Oracle Data Guard cluster and applies only to AS3000 Network Gateway and Archive Server stations.

To update odbc.ini after upgrading an AS3000 Network Gateway or Archive Server

1. On an AS3000 Network Gateway or Archive Server station, log in as the **root** user.
2. Change to the **/usr/mvf/odbc32v52** directory.
3. In a text editor, open the **odbc.ini** file.
4. In the [MVF] section, update the AlternateServers attribute (it may be initially blank) with the standby server name (a fully qualified domain name may be used). For example:

   ```
   AlternateServers=(Hostname=sopron:PortNumber=1521:SID=MVF)
   ```

5. Save the file and close it.

After updating the file, no reboot is necessary.

6. Repeat the steps for any other AS3000 Network Gateway or Archive Server station.

2. Migrating a cache volume from a flat to a hierarchical structure

(Topic number: 102251)

Note:

If upgrading from IMPAX 6.5, the caches may have already been migrated to a hierarchical structure; this task can then be skipped.

Before starting the migration, verify the condition of the caches:

1. Install the MVFcachecheck package.
2. Run the mvf-clean-cache tool.
3. If the mvf-clean-cache output indicates that there are problems, resolve them.

IMPAX stores DICOM objects in cache so that they can be displayed, transmitted to other DICOM devices, and archived. Prior to IMPAX 6.5, the cache structure was flat (each cache volume contained one directory), which limited the cache size because once a certain number of objects are in the directory, access to the cache can become very slow. Large sites may resolve this by deploying numerous cache volumes, which can be difficult to manage.

As of IMPAX 6.5, a hierarchical cache structure is supported for image and web caches, permitting larger cache volumes. The old flat cache structure continues to be supported; only new images arriving in the system or existing images retrieved from archive are written to cache using the hierarchical structure. However, the cache migration tool allows a site to migrate its existing caches if it would like to immediately take advantage of the hierarchical structure.

Note:

The cache migration tool is included in the MVFCache (Windows) and IMPAXmvfc (Solaris) packages, which are part of the standard IMPAX install packages.

To migrate a cache volume from a flat to a hierarchical structure

1. At a command prompt on the system where the cache volume is local, type

   cache_migration.exe *parameters* (Windows)

   or

   cache-migration *parameters* (Solaris, logged in as mvf user)

   where *parameters* are as follows:

Parameters	Values	Default value
-S	The cache volume to migrate from. If a source_volume_ref is not specified, you are prompted to choose from a list. If the destination volume is different from the source volume, make sure that the source cache volume is closed before running the cache-migration tool. When closed, new images cannot be received by this volume, which will likely be removed after the migration. To close the cache volume, start the CLUI tool and type **cache close *volume_ref***	Not applicable
-D	The cache volume to migrate to. It can be the same as the source volume. There should be enough space in the destination volume for all the studies in the source volume. If a destination_volume_ref is not specified, you are prompted to choose from a list.	Not applicable
-X	***number***—The delay in seconds before the original files are deleted. If not specified, the original files are not deleted. If 0, the original files are deleted immediately.	Not applicable
-F	***number***—The maximum number of cache files to be handled by each thread in the application; a performance-tuning parameter.	`100`
-T	***number***—The number of threads to handle the copying of files; a performance-tuning parameter.	`3`
-I	***number***—How often to report on the progress of the migration, in minutes.	`5`
-f	***log_file***—Log file name.	Not applicable

Tip:

Use the **-?** parameter to view usage or help information.

Example:

```
cache_migration.exe -F 500 -T 4 -I 2 -f migration.log
List of eligible cache volumes
1000 : /cache/mvfcache
1001 : /cache/vcacheRSNA2003
1002 : /cache/newcache
Source volume_ref? 1000
Destination volume_ref? 1000
Delete original files (Y/N)? y
How long to wait to delete (sec)? 10
```

After the migration, verify the condition of the caches:

1. Run the mvf-clean-cache tool.

2. If the mvf-clean-cache output indicates that there are problems, resolve them.

For details about configuring the cache directory structure, see "Configuring the hierarchical cache directory structure" (topic number 102687) in the *IMPAX 6.5.1 Server Knowledge Base*.

3. Restarting SMMS server alerts

(Topic number: 58318)

After the database has been upgraded or restored, you can restart SMMS (if applicable).

To restart SMMS server alerts

1. On the SMMS server, double-click the **Enable GSC Notifications** icon.
2. Open the file **C:\agfa\config\emailcmd.cfg** for editing.
3. Change the line `enabled = 'false'` to **enabled** = **'true'**.
4. Save the file and close it.

Alerts can now be sent about the Database Server.

4. Re-enabling IMPAX crontab entries

(Topic number: 58321)

After the database has been upgraded or restored, you can re-enable the IMPAX crontab entries.

To re-enable IMPAX crontab entries

1. Log into the Database Server as the **oracle** or **service** user.
2. To open the crontab file, type **crontab -e**.
3. Locate all entries related to IMPAX that have been commented out.
4. Remove the # marks to re-enable these entries.
5. Save and close the file.

5. Re-enabling archive logging

(Topic number: 60399)

Archive logging was disabled during the Database Server upgrade. Re-enable it after the IMPAX upgrade.

To re-enable archive logging

1. Log into the Database Server as the **oracle** user.

2. Type the following commands:

   ```
   mvf@os1spar:/usr/mvf$ sqlplus /nolog
   SQL> connect /as sysdba
   SQL> shutdown immediate
   SQL> startup mount exclusive
   SQL> alter database archivelog;
   SQL> alter database open;
   SQL>  archive log list;
   SQL> exit;
   ```

Archive logging is enabled.

6. Performing a warm backup of the database

(Topic number: 15588)

After all database data and software are upgraded or restored, reconfigure and perform a warm backup of the database.

To perform a warm backup of the database

1. Log into the Database Server as the **oracle** user.
2. If backing up to tape, record the date on the tape jacket and insert the tape into the tape drive.
3. Change to the **/usr/mvf** directory.
4. To reconfigure the database, type

   configure_backup

   Note:

   You must rerun this command after upgrading from all versions of IMPAX. For more details on using this command, refer to “Configuring backups to disk” (topic number 8904) or “Configuring backups using Flashbackup on Solaris” (topic number 66399) in the *IMPAX 6.5.1 Server Knowledge Base*.

5. Type **runbackup**

The backup may take a significant amount of time.

If you ever need to restore the database from a backup, follow the instructions in the Oracle Server component of the *IMPAX 6.5.1 Server Knowledge Base*.

7. Generating the portable password file

(Topic number: 58324)

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

When installing IMPAX AS3000 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. This file is also needed by the Curator and Application Server components, and by AS300 Network Gateway and Archive Servers (if used).

To generate the portable password file

1. Log into the AS3000 Database Server 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. Use a password that you will remember.
4. To copy the portable password file from the Database Server to the target server, type

   scp /usr/mvf/mvf.portable.psd service@*target_host_name*:/usr/mvf/mvf.portable.psd

   where *target_host_name* is the host name of the server where the password file is needed.
5. When you are finished copying the password file to the target servers, delete /usr/mvf/mvf.portable.psd from the Database Server.

8. Installing license keys on AS3000 servers

(Topic number: 60536)

IMPAX 6.2 or later license key files can be backed up and reused for all Network Gateway and Archive Server stations. MVF license keys must be installed on each single-host and Network Gateway station. Archive license keys must be installed on each single-host, Archive Server/Network Gateway, and Archive Server station.

Installing the mvf license key on a Solaris server

(Topic number: 58053)

MVF license keys must be installed on each single-host, Archive Server/Network Gateway, and Network Gateway station.

To install the mvf license key on a Solaris server

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. Change to the **/usr/mvf** directory.
3. Copy the license key file to the mvf directory on the hard drive.
4. Rename the license key file to:

   mvf.lic

Installing the archive license key on a Solaris server

(Topic number: 58056)

Archive license keys must be installed on each single-host, Archive Server/Network Gateway, and Archive Server station.

To install the archive license key on a Solaris server

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. Change to the **/usr/mvf** directory.
3. Copy the license key file to the mvf directory on the hard drive.
4. Rename the license key file to:

   mvfarch.lic

9. Installing and starting Compressor

(Topic number: 10168)

If lossy compression was not enabled when IMPAX was installed, and you want to enable it now, you must manually install and start the Compressor Scheduler package on the Database Server (or single-host server). For instructions, refer to "Installing Compressor Scheduler manually on Solaris" (topic number 6969) in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

The Compressor files are already installed on those systems with the IMPAXmvfc package (such as Network Gateways and Archives); however, Compressor is not actively running and must be manually

started, if required. For instructions, refer to “Starting Compressor manually on Solaris” (topic number 6925) in the *IMPAX 6.5.1 AS3000 Installation and Configuration Guide*.

Upgrading Windows components to IMPAX 6.5.1

8

The IMPAX 6.2 or later cluster includes various Windows-based servers, such as the Application Server and Curator, that also must be upgraded to IMPAX 6.5.1.

1. Upgrading external software on Windows-based servers

(Topic number: 60466)

Note:

If upgrading an AS3000 cluster from IMPAX 6.5 to IMPAX 6.5.1, it is not necessary to upgrade the Windows components and Oracle Client for Windows. You can skip ahead to *Upgrading AS300 Network Gateway and Archive Server stations* (refer to page 90).

To function correctly with IMPAX 6.5.1, some of the Windows components and Oracle Client for Windows software must be upgraded. Perform these tasks on all Windows-based servers, including any AS300 Archive Servers and Network Gateways, the Application Server, and Curator, but not on the IMPAX Client stations.

Upgrading Windows Server 2003 to Windows Server 2003 SP2

(Topic number: 47207)

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

CAUTION!

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

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

To upgrade Windows Server 2003 to Window Server 2003 SP2

1. Connect to the network or computer where you want to create the distribution folder.
2. In the shared folder, create a distribution folder for the service pack.
3. Copy WindowsServer2003-KB914961-SP2-*XXX*-*LLL*.exe into the distribution folder.
4. Open a command prompt.
5. To extract the files, type the following:

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

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

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

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

Determining the version of the installed Oracle Client

(Topic number: 106578)

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

Important!

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

To determine the version of the installed Oracle Client

1. Open a command prompt.
2. Type

   sqlplus -V

If the command returns `SQL*Plus: Release 10.2.0.1.0 - Production`, version 10.2.0.1 is installed and needs to be uninstalled first. For further details, see *Removing ODBC entries prior to uninstalling the Oracle Client* (refer to page 103) and *Uninstalling the previous version of Oracle Client* (refer to page 103)

If the command returns `SQL*Plus: Release 10.2.0.4.0 - Production`, version 10.2.0.4 is installed and needs to be upgraded. For further details, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 107).

Uninstalling the previous version of Oracle Client

(Topic number: 65367)

CAUTION!

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

To export all or part of the registry to a text file

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

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

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

To uninstall the previous version of Oracle Client

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

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

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

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

Installing and configuring the Oracle 10g Client for Windows

(Topic number: 6790)

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

Determine which Oracle Client is installed on the system; see *Determining the version of the installed Oracle Client* (refer to page 102). If Oracle Client version 10.2.0.1 is installed, uninstall it. If Oracle Client version 10.2.0.4 is installed, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 107).

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.

Upgrading to the 10.2.0.4 version of the Oracle Client for Windows

(Topic number: 106600)

Important!

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

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

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

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

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

The Oracle Client is upgraded.

Setting up a connection to the Oracle database

(Topic number: 46341)

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

To set up a connection to the Oracle database

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

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

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

    or

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

Reconfiguring ODBC data source names

(Topic number: 67665)

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

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

To reconfigure ODBC data source names

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

   where *Oracle_instance_name* is the name typed when *Installing and configuring the Oracle 10g Client for Windows* (refer to page 104).
6. Click **Finish**.
7. In the Data Source Name field, type **mvf**.
8. Type a description, if needed.
9. In the TNS Service Name field, type **MVF.world**.
10. In the User Name field, type **mvf**.

    The user ID must be lowercase.
11. To save the changes and close the dialog, click **OK**.
12. To save the new sources and exit the ODBC Data Source Administrator dialog, click **OK**.
13. If reconfiguring the Application Server, repeat the previous steps for the **mvf_ora** DSN as well.

Upgrading to Internet Explorer 7

(Topic number: 47486)

We recommend that you upgrade all Windows 2003 IMPAX servers running earlier versions of Internet Explorer to Internet Explorer 7. To verify which version of Internet Explorer is being used, start Internet Explorer and select **Help** > **About Internet Explorer**. This procedure is not required for Windows 2008 server, as Internet Explorer 7 is included with Windows 2008 server.

To upgrade to Internet Explorer 7

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

http://www.microsoft.com/windows/internet-explorer/ie7/

3. From this page, you can either download Internet Explorer 7 or order it on CD.
4. Once you have obtained the software, run it on each server that needs upgrading.
5. To install the software, follow the on-screen prompts.

2. Upgrading AS300 Network Gateway and Archive Server stations

(Topic number: 60463)

If using AS300 (Windows-based) Network Gateway or Archive Server stations at your site, these must be upgraded to IMPAX 6.5.1 as well.

Retrieving the portable password file from the target server

(Topic number: 58327)

The portable password file synchronizes passwords between components. The file contains all of the user IDs and passwords for all default IMPAX users.

To retrieve the portable password file from the target server

1. On the server (Application Server, Curator, Network Gateway, or Archive Server), open a command prompt.
2. Type

   scp service@*target_host_name*:/usr/mvf/mvf.portable.psd /cygdrive/c/mvf.portable.psd

   where *target_host_name* is the host name of the Database Server where the portable password was generated.
3. Exit the command prompt.

Uninstalling the IMPAX software

(Topic number: 6743)

Before upgrading an existing server to IMPAX 6.5.1, you must uninstall the previous release of the IMPAX software packages and Knowledge Bases.

Recording the names of previously installed IMPAX AS300 software packages

(Topic number: 29655)

Before uninstalling the AS300 server packages for the previous release of IMPAX, record the package names. It is useful to know these before installing IMPAX 6.5.1.

The procedure for locating the package names differs depending on what version you are upgrading from.

To record the names of previously installed IMPAX 6.4 or later AS300 software packages

1. On the IMPAX 6.4 or later server, open Control Panel.
2. Select **Add or Remove Programs**.
3. Select **AGFA IMPAX AS300** and click **Change**.
4. After the installer launches, click **Modify**.
5. Click **Next**.
6. Make note of the installed packages.

To record the names of previously installed IMPAX 6.2 or 6.3 AS300 software packages

1. On the IMPAX 6.2 or 6.3 Windows server to upgrade, select **Start** > **Run**.
2. In the Open field, type **regedit** and click **OK**.
3. In the Registry Editor, select **HKEY_LOCAL_MACHINE\SOFTWARE\Mitra Imaging Inc.** and **HKEY_LOCAL_MACHINE\SOFTWARE\Mitra** and make note of the installed packages (refer to page 91).

IMPAX packages found in the registry

(Topic number: 58575)

The following are IMPAX 6.2 or 6.3 packages that may be found in the registry. You may see some or all of these packages, depending on your configuration and the version of IMPAX installed. As of IMPAX 6.4, packages are listed in Control Panel instead.

Note:

As of IMPAX 6.5, Scavenger Manager is no longer supported.

Default packages	Location in HKEY_LOCAL_MACHINE\SOFTWARE\
MVFCore	Mitra Imaging Inc.\MVF Core v*number*
MVFCache	Mitra Imaging Inc.\MVF Cache v*number*
MVFSqlserver	Mitra Imaging Inc.\MVF SQLServer Extensions v*number*
MVFNetworkGateway	Mitra Imaging Inc.\MVF Network Gateway v*number*
AdministrationTools	Mitra\AdministrationTools
MVFocr	Mitra Imaging Inc.\MVF Ocrv*number*

Archive packages	Location in HKEY_LOCAL_MACHINE\SOFTWARE\
MVFjdlt	Mitra Imaging Inc.\MVF JDLT v*number*
MVFjdvd	Mitra Imaging Inc.\MVF JDVD v*number*

Archive packages	Location in HKEY_LOCAL_MACHINE\SOFTWARE\
MVFscdr	Mitra Imaging Inc.\MVF SCDR v*number*
MVFhsm	Mitra Imaging Inc.\MVF HSM Archive v*number*
MVFsdlt	Disregard if found; not required for IMPAX 6.5.1.

Optional packages	Location in HKEY_LOCAL_MACHINE\SOFTWARE\
MVFCompressor	Mitra Imaging Inc.\MVF Compressor v*number*
MVFScavenger	Mitra Imaging Inc.\MVF Archive Scavenger v*number*
MVFCurator	Mitra Imaging Inc.\MVF Curator v*number*
MVFcdexport	Mitra Imaging Inc.\MVF CD Export v*number*
MVFpap	Mitra Imaging Inc.\MVF PACS Archive Provided v*number*

Make note of the installed packages so that you can select the same ones when installing IMPAX 6.5.1.

Uninstalling the previous IMPAX software packages

(Topic number: 6744)

If you are upgrading an existing server, before installing the IMPAX 6.5.1 AS300 server packages, uninstall the previous-version IMPAX packages.

To uninstall the previous IMPAX software packages

1. Open Control Panel.
2. Select **Add or Remove Programs**.
3. Under Currently installed programs, select **Agfa IMPAX 6.2 *version***, **Agfa IMPAX 6.3 *version***, or **Agfa IMPAX AS300** (used for IMPAX 6.4 and later).
4. Click **Change/Remove**.

   or

   For uninstalling IMPAX 6.4 and later, click **Remove**.
5. When prompted, type your name (minimum three characters). Click **Next**.
6. In the Confirmation dialog, click **OK** or **Yes**.
7. On the Maintenance Complete screen, click **Finish**.
8. Restart the server.

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

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).

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 92).

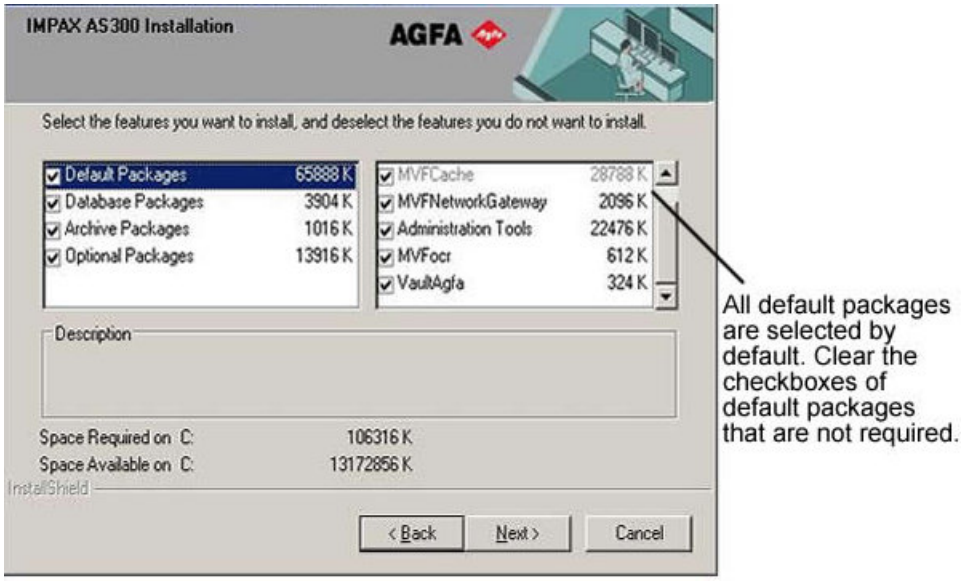
To install the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages

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.

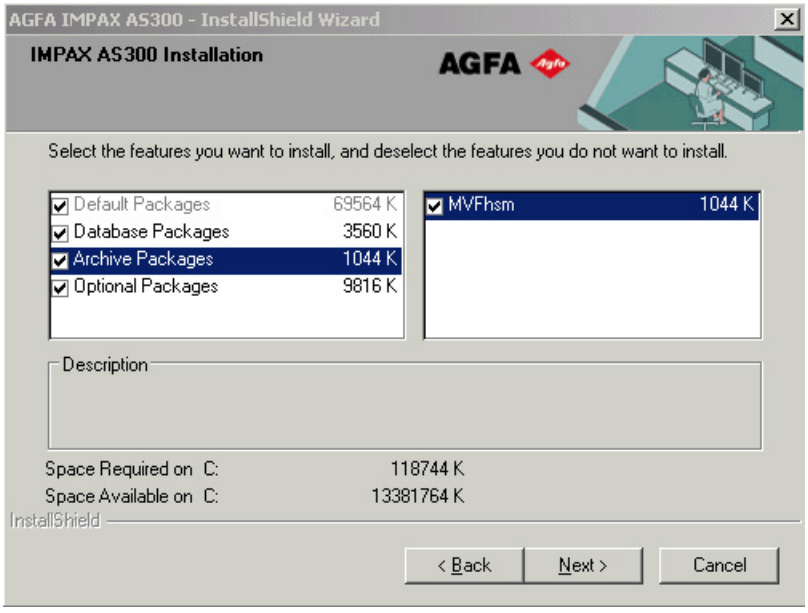
   If installing a Network Gateway or an Archive Server/Network Gateway combination, you can normally leave all the default packages selected.

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

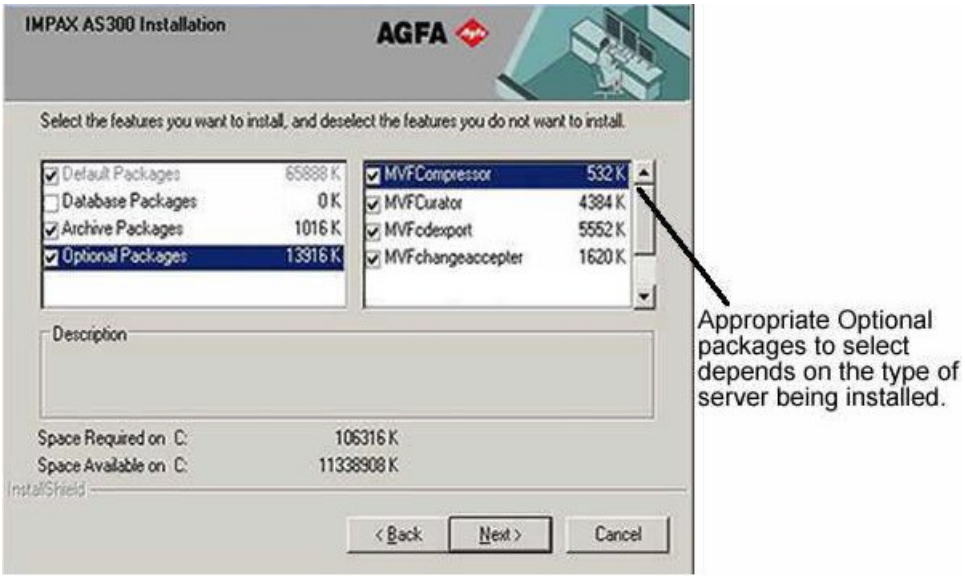


6. Clear the **Database Packages** checkbox.
7. For Archive Servers, select the **Archive Package** label. The MVFhsm is the only archive package listed and is selected by default. If not using an HSM archive, clear the **MVFhsm** checkbox; otherwise, keep it selected.

   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.

Installing and configuring Store and Remember archiving

(Topic number: 15546)

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).

Some sites may want to have their studies mirrored at another site through PACS Store and Remember archiving. This mirroring protects against loss of data and allows studies from one PACS to be viewed at another. This can be achieved effectively using the PACS Archive Provider (PAP).

For instruction on installing and configuring a PACS Archive Provider, refer to "Configuring a PACS Archive Provider (PAP)" (topic number 11586) in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

3. Upgrading the Application Server from a previous version

(Topic number: 11188)

Important!

For AS300 Oracle and for all AS3000 (Solaris server) sites, before upgrading the Application Server, ensure that you have the correct version of Oracle 10g Client installed. For instructions on how to check the current version of the Oracle Client, see *Determining the version of the installed Oracle Client* (refer to page 102). For instructions on how to install the Oracle 10g Client, see *Installing and configuring the Oracle 10g Client for Windows* (refer to page 104).

Upgrade all Application Servers in the cluster to IMPAX 6.5.1.

Important!

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

Upgrading the ADAM database

(Topic number: 58664)

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

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

If you are upgrading a cluster to Windows Server 2008, you must replicate the ADAM database instance on a new Windows 2008 server, which uses the AD LDS database. For information on how to replicate the ADAM database on a Windows 2008 server, see *Migrating an Application Server from a Windows 2003 server to a Windows 2008 server* (refer to page 120).

Backing up the ADAM database

(Topic number: 6717)

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

To back up the ADAM database

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

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

    or

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

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

Stopping services on the Application Servers

(Topic number: 10144)

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

To stop services on the Application Servers

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

Uninstalling IMPAX 6.2 documentation

(Topic number: 10736)

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

To uninstall the IMPAX 6.2 documentation

1. Open Control Panel.
2. Select **Add or Remove Programs**.
3. Under Currently installed programs, select **IMPAX 6.2 Documentation**.
4. Click **Change/Remove**.

5. In the Confirmation dialog, click **OK**.
6. In the Maintenance Complete dialog, click **Finish**.
7. Under Currently installed programs, select **IMPAX Application Server Knowledge Base**.
8. Click **Change/Remove**.
9. In the Confirmation dialog, click **OK**.
10. In the Maintenance Complete dialog, click **Finish**.
11. Under Currently installed programs, select **Impax Client Knowledge Base**.
12. Click **Change/Remove**.
13. In the Confirmation dialog, click **OK**.
14. In the Maintenance Complete dialog, click **Finish**.
15. Under Currently installed programs, select **IMPAX Server Knowledge Base**.
16. Click **Change/Remove**.
17. In the Confirmation dialog, click **OK**.
18. In the Maintenance Complete dialog, click **Finish**.

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

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

To uninstall IMPAX 6.3 or later documentation

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

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

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

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

To uninstall the IMPAX Installation Server

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

The Agfa IMPAX Installation Server is uninstalled.

Installing the recommended version of the Oracle Client

(Topic number: 106750)

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

Important!

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

Determining the version of the installed Oracle Client

(Topic number: 106578)

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

Important!

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

To determine the version of the installed Oracle Client

1. Open a command prompt.
2. Type

   sqlplus -V

If the command returns `SQL*Plus: Release 10.2.0.1.0 - Production`, version 10.2.0.1 is installed and needs to be uninstalled first. For further details, see *Removing ODBC entries prior to uninstalling the Oracle Client* (refer to page 103) and *Uninstalling the previous version of Oracle Client* (refer to page 103)

If the command returns `SQL*Plus: Release 10.2.0.4.0 - Production`, version 10.2.0.4 is installed and needs to be upgraded. For further details, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 107).

Removing ODBC entries prior to uninstalling the Oracle Client
(Topic number: 119055)

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

To remove ODBC entries prior to uninstalling the Oracle Client

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

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

Uninstalling the previous version of Oracle Client
(Topic number: 65367)

CAUTION!

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

To export all or part of the registry to a text file

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

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

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

To uninstall the previous version of Oracle Client

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

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

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

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

Installing and configuring the Oracle 10g Client for Windows
(Topic number: 6790)

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

Determine which Oracle Client is installed on the system; see *Determining the version of the installed Oracle Client* (refer to page 102). If Oracle Client version 10.2.0.1 is installed, uninstall it. If Oracle Client version 10.2.0.4 is installed, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 107).

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.

Setting up a connection to the Oracle database

(Topic number: 46341)

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

To set up a connection to the Oracle database

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

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

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

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

    or

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

Reconfiguring ODBC data source names

(Topic number: 67665)

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

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

To reconfigure ODBC data source names

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

   where *Oracle_instance_name* is the name typed when *Installing and configuring the Oracle 10g Client for Windows* (refer to page 104).
6. Click **Finish**.
7. In the Data Source Name field, type **mvf**.
8. Type a description, if needed.
9. In the TNS Service Name field, type **MVF.world**.
10. In the User Name field, type **mvf**.

    The user ID must be lowercase.
11. To save the changes and close the dialog, click **OK**.
12. To save the new sources and exit the ODBC Data Source Administrator dialog, click **OK**.
13. If reconfiguring the Application Server, repeat the previous steps for the **mvf_ora** DSN as well.

Upgrading to the 10.2.0.4 version of the Oracle Client for Windows
(Topic number: 106600)

Important!

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

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

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

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

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

The Oracle Client is upgraded.

Upgrading the IMPAX Application Server software to 6.5.1
(Topic number: 9863)

Important!

Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

After backing up the ADAM database (refer to page 99), you can upgrade the Application Server software.

Note:

This installation does not overwrite the existing ADAM database.

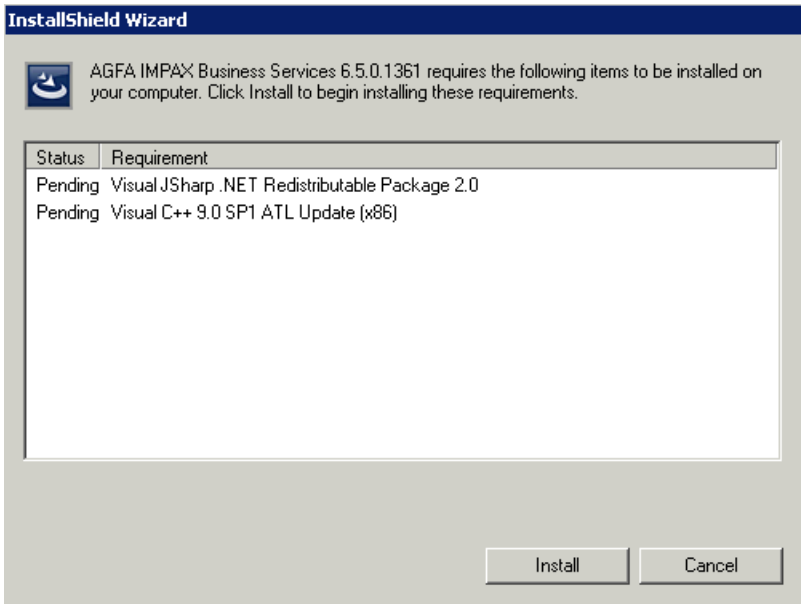
To upgrade the IMPAX Application Server software to 6.5.1

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

The following packages are installed on the Application Server prior to the upgrade.

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

  If any of these packages are listed in the InstallShield Wizard dialog, they are installed when you click **Install**. If any of these packages do not appear in the list, those packages are already installed on the machine.



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

   For example, set the path to J:\wwwroot rather than C:\inetpub\wwwroot.
9. Click **Next**.
10. On the Setup Type screen, select **Custom**. Click **Next**.
11. If you have an IMPAX RIS to connect to, click **RIS Web Services** and select **This feature will be installed on local hard drive**.
12. If you are using SmartCard authentication, verify that **NHS SmartCard Web Services** is selected. If it is not selected, select it. Select **This feature will be installed on local hard drive**.
13. Click **Next**.
14. Click **Install**.

15. On the InstallShield Wizard Completed screen, select **Launch IMPAX Business Services Configuration tool**. Click **Finish**.
16. When the message `Previous configuration found from version 6.X.X...` appears, click **Yes**. This message is not displayed when upgrading from IMPAX 6.5 to IMPAX 6.5.1.
17. In the Configuration Tool, click **Apply**.
18. To close the Configuration Tool, click **OK**.

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 100). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 114).

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

To install the IMPAX documentation

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

   A `Preparing to install` message appears.
3. On the Welcome screen, click **Next**.
4. On the Setup Type screen, select the appropriate option and click **Next**.
   - To install all documentation in all available languages (up to 24 languages), select **All Documentation**.
   - To install all English-language documentation, select **All English Documentation**. This is the default.
   - To select which documentation to install in which languages, select **Select Documentation to Install**.
5. If you selected Select Documentation to Install, on the Choose Features screen, you can select particular Knowledge Bases or languages to install.
   - To install the IMPAX Client Knowledge Base in two or more languages, click  beside the name of the language to install and select **This feature will be installed on the local hard drive**. (Note that English must be installed.)

- To **not** install the IMPAX Server, IMPAX Application Server, or IMPAX Client documentation, click  beside the appropriate label and select **This feature will not be available**.

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

   Installation progress messages are displayed.

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

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

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 118)) or on a separate, dedicated Windows-based server.

Note:

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

Therefore, we recommend:

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

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

The Installation Server Setup package contains:

- The installers (or links) for the IMPAX Client prerequisites:
  - .NET Framework 3.5 SP1
  - Visual C++ 9.0 SP1
  - DirectX

- The IMPAX Client Installer
- A web page with links to:
  - IMPAX Client system requirements
  - IMPAX Client installation instructions (available in 19 languages)
  - Links to the IMPAX Client Installer
  - Links to the individual perquisites

Running the IMPAX Installation Server package
(Topic number: 7758)

CAUTION!

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

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

To run the IMPAX Installation Server package

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

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

   or

   To install the application to another location, click **Change**. In the Change Current Destination Folder dialog, browse for the directory location to install into and click **OK**. On the Destination Folder screen, click **Next**.
4. On the Ready to Install the Program screen, click **Install**.

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

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

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

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

(Topic number: 11405)

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

Note:

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

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

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

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

   or

   If Healthcheck has been configured to automatically log in, type

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

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

CAUTION!

Setting the refresh interval below five seconds impacts performance.

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

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

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

Upgrading additional Application Servers in the cluster
(Topic number: 11210)

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

To upgrade additional Application Servers in the cluster.

1. Upgrade the IMPAX Application Server software (refer to page 107).
2. Verify the installation.

Upgrading the AD LDS database from IMPAX 6.5 to IMPAX 6.5.1
(Topic number: 130063)

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

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

Creating a one-time backup of AD LDS
(Topic number: 113662)

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

Backing up the AD LDS database at this time is important in the event that user migration fails.

Follow this procedure to create a one-time backup of the AgfaHealthcare AD LDS instance.

To create a one-time backup of AD LDS

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

   dsdbutil
3. At the dsdbutil prompt, type

   activate instance AgfaHealthcare
4. At the dsdbutil prompt, type

   ifm
5. At the ifm prompt, type

   create full *location*

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

Example:

ifm: create full C:\Backup\AgfaHealthcare

6. At the ifm prompt, type

   quit

   At the dsdbutil prompt, type

   quit

The AD LDS instance is backed up.

Stopping services on the Application Servers

(Topic number: 10144)

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

To stop services on the Application Servers

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

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

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

To uninstall IMPAX 6.3 or later documentation

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

3. In the Programs and Features dialog, under Currently installed programs, select **AGFA IMPAX *version* Knowledge Base *buildnumber* Documentation**.
4. Click **Remove**.
5. In the confirmation dialog, click **OK**.

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

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

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

To uninstall the IMPAX Installation Server

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

The Agfa IMPAX Installation Server is uninstalled.

Upgrading the IMPAX Application Server software to 6.5.1

(Topic number: 126080)

Important!

Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

After backing up the ADAM database (refer to page 99), you can upgrade the Application Server software.

Note:

This installation does not overwrite the existing ADAM database.

To upgrade the IMPAX Application Server software to 6.5.1

1. Insert the IMPAX Business Services CD.

2. Navigate to the CD ROM drive, which contains the Business Services software.
3. Click **Install**.
4. On the Welcome screen, click **Next**.
5. On the license agreement screen, select **I accept the terms in the license agreement**. Click **Next**.
6. On the Web Services Installation Folder screen, click **Change**.
7. Set the path to the **wwwroot** directory so that it matches the pre-upgrade installation location. Click **OK**.

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

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 100). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 114).

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

To install the IMPAX documentation

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

   A `Preparing to install` message appears.

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

   Installation progress messages are displayed.
7. On the InstallShield Wizard Completed screen, click **Finish**.

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

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 118)) or on a separate, dedicated Windows-based server.

Note:

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

Therefore, we recommend:

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

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

The Installation Server Setup package contains:

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

Running the IMPAX Installation Server package
(Topic number: 7758)

CAUTION!

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

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

To run the IMPAX Installation Server package

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

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

or

To install the application to another location, click **Change**. In the Change Current Destination Folder dialog, browse for the directory location to install into and click **OK**. On the Destination Folder screen, click **Next**.

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

   The first installer runs.

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

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

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

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

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

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

(Topic number: 11405)

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

Note:

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

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

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

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

   or

   If Healthcheck has been configured to automatically log in, type

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

To	Append	Example
View the results in HTML	**?format=html** to the end of the URL	**https://appserver.hospital.com/AgfaHC.Healthcheck.Escrow/EscrowForm.aspx?format=html**

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

CAUTION!

Setting the refresh interval below five seconds impacts performance.

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

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

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

Upgrading additional Application Servers in the cluster

(Topic number: 11210)

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

To upgrade additional Application Servers in the cluster.

1. Upgrade the IMPAX Application Server software (refer to page 107).
2. Verify the installation.

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

(Topic number: 109634)

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

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

For complete instructions on how to migrate ADAM data from Windows 2003 to Windows 2008, consult the IMPAX 6.5.1 *Application Server Installation, Upgrade and Configuration Guide*.

4. 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*.

5. Upgrading the Curator

(Topic number: 59657)

All dedicated Curator stations need upgrading. Upgrade the master Curator first, by uninstalling the existing IMPAX software, then installing the IMPAX 6.5.1 AS300 software with the MVFCore, possibly MVFCache, MVFCurator, and MVFcdexport packages selected. Then upgrade all slave Curators in much the same way, except that the MVFcdexport package only has to be included on one of the slave Curators.

Uninstalling the previous IMPAX software packages

(Topic number: 6744)

If you are upgrading an existing server, before installing the IMPAX 6.5.1 AS300 server packages, uninstall the previous-version IMPAX packages.

To uninstall the previous IMPAX software packages

1. Open Control Panel.
2. Select **Add or Remove Programs**.
3. Under Currently installed programs, select **Agfa IMPAX 6.2 *version***, **Agfa IMPAX 6.3 *version***, or **Agfa IMPAX AS300** (used for IMPAX 6.4 and later).
4. Click **Change/Remove**.

   or

   For uninstalling IMPAX 6.4 and later, click **Remove**.
5. When prompted, type your name (minimum three characters). Click **Next**.
6. In the Confirmation dialog, click **OK** or **Yes**.
7. On the Maintenance Complete screen, click **Finish**.
8. Restart the server.

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

Installing the Curator and CD Export server software

(Topic number: 7047)

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

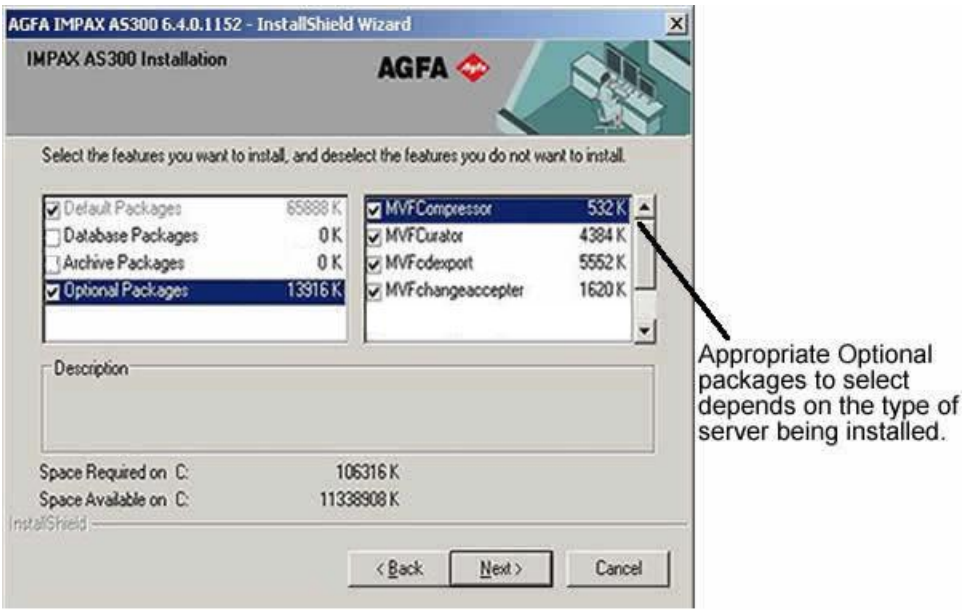
You can now install the AS300 software with the appropriate packages. If installing multiple Curators, install and configure the master Curator before installing the secondary ones.

To install the Curator and CD Export server software

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. Clear the **Database Packages** checkbox.
6. Clear the **Archive Packages** checkbox.
7. Select the **Optional Packages** label and select the appropriate packages. **MVFCurator** must stay selected. **MVFcdexport** is also required except, perhaps, on slave Curators.

Normally, no other optional packages are required, so you can clear other selected checkboxes. In particular, clear the **MVFchangeacceptor** checkbox and do **not** select the **MVForadg** checkbox.



8. Click **Next**.
9. Browse to the location of the portable password file and click **OK**.
10. Type the temporary password used to create the portable password file and click **Next**.

    The mvf.psd file is imported under C:\mvf.
11. On the Summary screen, click **Next**.

    The files are copied.
12. 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.

6. Upgrading Clients to IMPAX 6.5.1

(Topic number: 10176)

IMPAX Clients, both local and remote, are used to view study images. The Client software can be installed on any appropriate, networked workstation and be used by anyone who has a valid license. At least one Client should be upgraded to IMPAX 6.5.1 for migration testing purposes.

Important!

After upgrading IMPAX, you must enable any scheduled worklists to add them to the IMPAX 6.5.1 Client List area. In the List area, click **Worklists**. In the Active column next to the worklist, select the checkbox for each worklist to display, then press **Enter**. For more details, refer to "Adding worklists to the List area" (topic number 8433) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Manually uninstalling the IMPAX 6.2 or later Client software (optional)

(Topic number: 7752)

Important!

This procedure is optional. You should not have to uninstall the IMPAX 6.2 or later Client software prior to installing the IMPAX 6.5.1 Client software. However, if the IMPAX Client is installed on Windows Vista, we recommend uninstalling it prior to the installation of the new version.

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

To manually uninstall the IMPAX 6.2 or later Client software

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

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

Installing the IMPAX Client

(Topic number: 7776)

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

Note:

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

To install the IMPAX Client

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

   For information on setting up a Client installation server, refer to "*Installing the IMPAX Installation Server* (refer to page 117)" (topic number 7773) in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide* or the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

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

   A `Preparing to Install` message appears.

   If on Windows Vista, a cscript.exe prompt may appear. To run it, click **OK**.

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

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

   Note:

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

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

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

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

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

5. On the Welcome to the InstallShield Wizard for IMPAX Client screen, click **Next**.

6. On the License Agreement screen, read the license agreement. If you agree, select **I accept the terms in the license agreement**. Click **Next**.

7. To install the application into C:\Program Files\Agfa\IMPAX Client, on the Destination Folder screen, click **Next**.

   or

To install the application to another location, click **Change**. In the Change Current Destination Folder dialog, browse for the directory location to install into and click **OK**. On the Destination Folder screen, click **Next**.

8. On the IMPAX Application Server screen, in the Get or confirm application server name field, type the fully qualified domain name of the Application Server to use. Click **Next**.

   A *fully qualified domain name* is the full name of a system, including its local host name and complete domain name. For example, if the Application Server is called *radserver*, it is on the network domain called *radnet*, and radnet is within the *healthorg.com* domain, the name to type would be *radserver.radnet.healthorg.com*.

9. On the IMPAX Login Type screen, select the appropriate authentication method: Windows, IMPAX, or Smart Card.

   - **Windows Authentication**—Logs into IMPAX using the Windows session credentials after launching the IMPAX Client or logging in with a Windows smart card.
   - **IMPAX Authentication**—Logs into the IMPAX Client separately from Windows. (If unsure of which option to select, use **IMPAX Authentication**.)
   - **Smart Card Authentication**—Logs into the IMPAX Client with a smart card in the **National Health Service (NHS) environment only**.

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

    The program is installed.

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

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

Post-migration tasks and stabilization

9

Some additional tasks must be performed after the database, the servers, and the Clients are upgraded to IMPAX 6.5.1.

1. Redirecting studies to the production server

(Topic number: 10180)

Important!

This topic applies only when using an AS3000 traveling server as part of the upgrade and migration.

If necessary, you can now configure the modalities to redirect studies to the production server, rather than the traveling server. How studies are redirected is modality-specific and is not documented in this publication.

2. Migrating studies from the traveling server

(Topic number: 10188)

Important!

This topic applies only when using an AS3000 traveling server as part of the upgrade and migration.

Using the Administration Tools or CLUI, you can send the studies on the traveling server to the production server.

Transmitting studies using the Administration Tools

(Topic number: 58342)

Use the Administration Tools to send the studies on the traveling server to the production server.

To transmit studies using the Administration Tools

1. In Administration Tools, on the Daily tab, click **Study Manager**.
2. Search for studies, and from the results list, select the studies to transmit.
3. Click **Transmit**.
4. In the dialog, select the station you want to transmit the study to.
5. Click **Transmit**.

Creating SEND jobs using CLUI

(Topic number: 58345)

To complete the migration of studies from the traveling server, you can create SEND jobs using CLUI.

To create SEND jobs using CLUI

1. In CLUI, specify the list of studies to transfer with the following command:

   study send *study_ref_1 study_ref_2... study_ref_n destination*

   or

   Generate the list of studies to transfer with the following query:

   save_refs a select study_ref from dosr_study where *column* = *constraint*
2. Go to menu mode by typing **go menu**.
3. Select **1** for Study Manager, then **9** for Send.
4. At the prompt for the list of studies to process, enter **a** to reference the save_refs list of studies.
5. At the prompt for the destination, enter the destination.

3. Migrating a cache volume from a flat to a hierarchical structure

(Topic number: 102251)

Note:

If upgrading from IMPAX 6.5, the caches may have already been migrated to a hierarchical structure; this task can then be skipped.

Before starting the migration, verify the condition of the caches:

1. Install the MVFcachecheck package.
2. Run the mvf-clean-cache tool.
3. If the mvf-clean-cache output indicates that there are problems, resolve them.

IMPAX stores DICOM objects in cache so that they can be displayed, transmitted to other DICOM devices, and archived. Prior to IMPAX 6.5, the cache structure was flat (each cache volume contained one directory), which limited the cache size because once a certain number of objects are in the directory, access to the cache can become very slow. Large sites may resolve this by deploying numerous cache volumes, which can be difficult to manage.

As of IMPAX 6.5, a hierarchical cache structure is supported for image and web caches, permitting larger cache volumes. The old flat cache structure continues to be supported; only new images arriving in the system or existing images retrieved from archive are written to cache using the hierarchical structure. However, the cache migration tool allows a site to migrate its existing caches if it would like to immediately take advantage of the hierarchical structure.

Note:

The cache migration tool is included in the MVFCache (Windows) and IMPAXmvfc (Solaris) packages, which are part of the standard IMPAX install packages.

To migrate a cache volume from a flat to a hierarchical structure

1. At a command prompt on the system where the cache volume is local, type

   cache_migration.exe *parameters* (Windows)

   or

   cache-migration *parameters* (Solaris, logged in as mvf user)

   where *parameters* are as follows:

Parameters	Values	Default value
-S	The cache volume to migrate from. If a source_volume_ref is not specified, you are prompted to choose from a list. If the	Not applicable

Parameters	Values	Default value
	destination volume is different from the source volume, make sure that the source cache volume is closed before running the cache-migration tool. When closed, new images cannot be received by this volume, which will likely be removed after the migration. To close the cache volume, start the CLUI tool and type **cache close *volume_ref***	
-D	The cache volume to migrate to. It can be the same as the source volume. There should be enough space in the destination volume for all the studies in the source volume. If a destination_volume_ref is not specified, you are prompted to choose from a list.	Not applicable
-X	***number***—The delay in seconds before the original files are deleted. If not specified, the original files are not deleted. If 0, the original files are deleted immediately.	Not applicable
-F	***number***—The maximum number of cache files to be handled by each thread in the application; a performance-tuning parameter.	`100`
-T	***number***—The number of threads to handle the copying of files; a performance-tuning parameter.	`3`
-I	***number***—How often to report on the progress of the migration, in minutes.	`5`
-f	***log_file***—Log file name.	Not applicable

Tip:

Use the **-?** parameter to view usage or help information.

Example:

```
cache_migration.exe -F 500 -T 4 -I 2 -f migration.log
List of eligible cache volumes
1000 : /cache/mvfcache
1001 : /cache/vcacheRSNA2003
1002 : /cache/newcache
Source volume_ref? 1000
Destination volume_ref? 1000
Delete original files (Y/N)? y
How long to wait to delete (sec)? 10
```

After the migration, verify the condition of the caches:

1. Run the mvf-clean-cache tool.
2. If the mvf-clean-cache output indicates that there are problems, resolve them.

For details about configuring the cache directory structure, see "Configuring the hierarchical cache directory structure" (topic number 102687) in the *IMPAX 6.5.1 Server Knowledge Base*.

4. Testing the installed software

(Topic number: 61185)

After installing the new version of IMPAX, perform certain tests to verify that the installation was successful.

To test the installed software

1. On the IMPAX Database Server, run the Administration Tools and ensure that you can log in using the administration password.
2. On the Application Server, open a web browser and connect to http://localhost. Ensure that the "Welcome to IMPAX" page is displayed.
3. Run the IMPAX Client and ensure that you can log in using the administration password.

5. Restarting antivirus software

(Topic number: 9916)

If you have antivirus software installed and have halted any scan jobs, restart the antivirus services.

To restart antivirus software

1. On a Windows server where scanning was stopped, launch the antivirus software.
2. Start the scan operation according to the vendor's instructions.

6. Restarting Connectivity Manager queues

(Topic number: 67610)

If Connectivity Manager is currently deployed, and you have stopped any queues, use the Queue Manager to restart them. Messages in a queue that is stopped are not processed and sit in the queue. Once the queue is restarted, messages are processed.

To restart Connectivity Manager queues

1. In the Connectivity Manager Service Tools, click **Queue Manager**.
2. In the Queue List table, select the checkbox beside the queue of any system device or real world device with a *DM Out* or *impax_report_server* Component.

   The Status of the queue should be Stopped.
3. Click **start**.

The Status of the queue changes to Started.

7. Taking a post-upgrade system snapshot

(Topic number: 6845)

After upgrading to IMPAX 6.5.1, use the migration_inventory tool to capture the state of the system to compare it with the previous IMPAX system. Perform this task on any computer on which the Migration Tools have been installed that can access the 6.5.1 Database Server.

To take a post-upgrade system snapshot

1. In a command prompt or terminal window, change to the directory containing the migration_inventory tool.
2. On a Windows server, type

   migration_inventory -s -d *database_name* -U *database_user_name* -P *database_password* -D *database_server_host_name*

   On a Solaris server, log in as mvf user and type

   ./migration_inventory -s -d *database_name* -U *database_user_name* -P *database_password* -D *database_server_host_name*

   The output is stored in the migration_info table. It lists the number of IMPAX studies, total objects, and objects in cache. It also lists all IMPAX source stations and DICOM printers.
3. To create a report file with this information, in Windows, type

   mig_reporter -t system_inventory_tool

   In Solaris, type

   ./mig-reporter -t system_inventory_tool

This command writes the output of the migration_inventory command to a report file in the /usr/mvf-mig6/reports or C:\mvf\mig6 directory. (For other parameters you can use with this command, refer to the appropriate version of the *IMPAX Preparing to Upgrade Guide*.)

8. Comparing pre- and post-upgrade snapshots

(Topic number: 6895)

Open the report file that contains the pre- and post-upgrade snapshot information. Compare the pre- and post-upgrade information. Ensure that all expected studies, objects, stations, and DICOM printers are still listed.

9. Installing the PSARMT and cache tools on a Solaris server

(Topic number: 40844)

The PSARMT and cache tools are on the AS3000 DVD.

To install the PSARMT and cache tools on a Solaris server

1. Log in as the **root** user.
2. Insert the IMPAX AS3000 DVD.
3. For the cache check and repair tools, navigate to the IMPAX_R6.5-*impax_build_label* directory.
4. To install the cache check and repair tools, type **pkgadd -d IMPAXcchk**.
5. When asked to select packages, to install all packages, press **Enter**.
6. When asked if you want to continue with the installation, type **y**.

   The tools are installed in the /usr/mvf/bin directory.
7. For the PSARMT Migration Tools, navigate to the IMPAX_R6.5-*impax_build_label* directory.
8. To install the PSARMT Migration Tools, type **pkgadd -d IMPAXsrmt**.
9. When asked to select packages, to install all packages, press **Enter**.
10. When asked if you want to continue with the installation, type **y**.

    The tools are installed in the /usr/mvf/bin directory.
11. Remove the IMPAX AS3000 DVD.

10. Running PSARMT to mark studies as PACS archived

(Topic number: 40850)

Important!

If the site does not use an external PACS, you can skip this topic.

The PACS Store and Remember Migration Tools enable a site to migrate from an external PACS system to IMPAX by allowing the external system to act as an archive server to IMPAX.

Run these commands on the upgraded IMPAX Database Server.

For more information regarding the configuration and execution of the PSARMT Migration Tools, refer to the PSARMT readme document, which can be found in the /usr/mvf-mig6 directory.

To run PSARMT to mark studies as PACS archived

1. Log in as the **mvf** or **service** user.
2. Change to the **/usr/mvf/bin** directory.
3. To build the PSARMT database tables in IMPAX, run **build-mvf-psarmt-database**.
4. Specify the migration configuration by running **mvf-psarmt-config-manager**. Parameters are as follows:
   - **-C *configuration_file_with_parameters*** Default is installed as mvf-psarmt.cfg. The attributes of this file are described in the PSARMT readme document.
   - **-R *study_status*** Retries studies with the given status for migration. Possible *study_status* values are conflict (C), error (E), and unknown (U). To retry all at once, specify -R EUC.
   - **-A {STOP | RESTART | KILL}** Performs the specified action command, one of STOP, RESTART, or KILL.
5. Perform the migration, based on the configuration defined in step 4, by running **mvf_psarmt**.

   This tool halts automatically when the migration is complete.
6. Update the missing information in the database from incoming study objects by running **mvf-study-fixer**.

At some later date, when studies are retrieved from the PACS, update the missing information in the database from incoming study object by running **mvf-study-fixer**.

Once the migration is complete and all studies have been fixed by the Study Fixer tool—this may be several months later—the PSARMT services halt automatically.

11. Detecting and correcting IMPAX cache corruption

(Topic number: 40853)

The Cache Check and Repair Tools are used to identify missing cache files and to repair or remove damaged ones. These tools are normally run across all of the cache file systems on the affected server, because files missing from a damaged cache can sometimes be found on another cache. Performance of the tools is hardware-dependent.

Checking the integrity and identity of cache files

(Topic number: 58348)

You can use the cache check and repair tools to check the integrity and identity of cache files against the IMPAX database.

To check the integrity and identity of cache files

1. Log in as the **oracle** user.

2. Change to the location of the cache check and repair tools.
3. Run **mvf-check-cache *parameters path_to_cache***

   where *parameters* can be one or more of the following:

   -i *seconds* Interval between display of progress messages. Default is every 10 seconds.

   -g Gentle cache check. Causes the tool to sleep every other second (and take twice as long).

   -m *mv_command_file* Path to the script of the mv commands which move problem files out of the cache directory and to a set of sibling directories on the same file system. Do not run this script on a damaged file system.

   -q A quick check of file existence only, and a simple file size sanity check. Cannot be used with the -m parameter.

For example:

mvf-check-cache -q /cache3/mvfcache

A report and additional diagnostic messages are written to the log file.

Note:

If the cluster has only one local cache, you can invoke the tool without arguments. If the cluster has multiple caches, you must specify the path to the cache on the command line. If a cache is not specified and multiple caches exist, the tool lists the cache paths and exits. Cache files that do not have locations registered in the database are not detected.

Finding files in a cache directory that are unknown to the database

(Topic number: 58351)

Files in the cache directory that contain invalid file name formats or are not registered in the database must be identified and possibly moved to another location.

To find files in a cache directory that are unknown to the database

1. Run **mvf-clean-cache *parameters path_to_cache***

   where *parameters* can be one or more of the following:

   - **-i *seconds***—Interval between display of progress messages on stderr. Default is every 10 seconds.
   - **-g**—Gentle cache check. Causes the tool to sleep every other second (and take twice as long).
   - **-m *mv_command_file***—Path to the script of the mv commands that move problem files out of the cache directory and to a set of sibling directories on the same file system. Do not run this script on a damaged file system.
   - **-v**—Increased verbosity. Causes all progress and report messages to be prefixed with the current date and time.

A report and additional diagnostic messages are written to the log file.

For example, run:

mvf-clean-cache -m move_cmds.sh /cache4/mvfcache

Moving the images from a cache directory

(Topic number: 58354)

You can move the images identified by the *mv_command_file*, which move problem files.

To move the images from a cache directory

1. Run the *mv_command_file*.

   For example, run **move_cmnds.sh**.

Generating a report of lost images

(Topic number: 58357)

This procedure is designed to be run on a server that has suffered damage to one or more cache file systems. This procedure generates a report of studies that contain DICOM object files that have been lost from a server's cache and deregisters the missing files from the database.

To generate a report of lost images

1. Run **mvf-report-loss *parameters report_file_name***

   where ***parameters*** can be one or more of the following:

   - **-i *seconds***—Interval between display of progress messages on stderr. Default is every 10 seconds.
   - **-g**—Gentle cache check. Causes tool to sleep every other second (and take twice as long).
   - **-r**—Run in deregister mode, changing the visible field values from `'C'` to `'F'` and permanently deleting all database locations for missing files. This action cannot be undone. It has no effect if the tool has never been run in marking mode.

Note:

If you omit the -r parameter, the tool runs in marking mode and checks all of the caches on the local server. If a file is missing, the visible field on the osr_location table is set to `'C'`, effectively making the file location "invisible". If a tool is rerun and files have since been restored to cache, the visible field values are set back to `"T"`. This is a default mode.

For example:

mvf-report-loss loss-report.txt

IMPAX system consistency is restored by deregistering missing cache files from the database.

Restoring leftover files to cache

(Topic number: 58360)

After performing a cache check and a cache clean, the leftover files must be restored to the cache. The following procedure analyzes the files to see if they are damaged, duplicates or incorrectly labeled, then restores the good files to the cache.

To restore leftover files to cache

1. Run **mvf-ddo-rescue *parameters files_or_directories_to_restore***

   where *parameters* can be one or more of the following:

   -c Disable DICOM object integrity checking, forcing the tool to assume that the object is valid.

   -i *seconds* Interval between display of progress messages on stderr. Default is every 10 seconds.

   -g Gentle cache check. Causes tool to sleep every other second (and take twice as long).

   -m *mv_command_file* Path to script of mv commands which restores good files by moving them to the cache they are missing from and renaming them as appropriate.

Note:

You can use any number of file and directory arguments. If the argument is a directory, the tool analyzes all the files in that directory and recursively analyzes all files in all subdirectories. At least one file or directory argument is required. Before running the move command script, ensure that you are at the root directory of each cache file system.

For example:

mvf-ddo-rescue -m move_cmds.sh old_lost_and_found

A report and additional diagnostic messages are written to the log file.

Reference: Where restored files are moved

(Topic number: 60216)

If the -m parameter is not used, restored files are moved to directories as follows:

./duplicates_for_deletion/

Valid DICOM files that are identical to (or are hard links to) files currently in cache on this server. Can be deleted.

./different_from_cache/

Valid DICOM files that have the same identification as files currently in cache, but are not identical to the files in cache. Can usually be safely deleted.

./non_local_objects/

Valid DICOM files that the database knows about, but are not currently supposed to be in cache on this server; copies of these files exist elsewhere in the system, on another server or stored in the archive. Can be deleted if there is full confidence in the integrity of the other copies.

./non_dicom_objects/

These files are not in DICOM format or are outside the size range for a DICOM file.

./corrupt_objects/

Damaged DICOM objects. These files have internal format problems or have been truncated. Probably nothing useful can be recovered from these files.

./cannot_identify/

These files may be damaged or they do not contain one of the fields needed to identify a file: SOP Instance UID, Transfer Syntax, Accession Number, Patient ID, and Series Instance UID.

./unregistered_objects/

Valid DICOM files that the database apparently has never heard of. These files failed the tool's identification method, probably because they originally failed HIS verification when received from the modality.

12. Uninstalling the IMPAX Migration Tools from a Windows computer

(Topic number: 47239)

Once all migration tasks and post-migration checks are completed, you must uninstall the IMPAX Migration Tools from all Windows-based computers on which they are installed. This is a legal requirement.

To uninstall the IMPAX Migration Tools from a Windows computer

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

   On Windows 2008 servers, select **Programs and Features**.
3. Select **IMPAX 6.5.1 AS300 Migration 6.5.0.*xxx***

   where *xxx* is the build number.
4. On Windows 2003 servers, click **Change/Remove**. On Windows 2008 servers, click **Uninstall**.
5. In the Confirm File Deletion dialog, click **Yes**.
6. At the Uninstall complete prompt, click **Finish**.

13. Uninstalling the IMPAX Migration Tools from a Solaris computer

(Topic number: 58426)

Once all migration tasks and post-migration checks are completed, you must uninstall the IMPAX Migration Tools from all Solaris-based computers on which they are installed. This is a legal requirement.

To uninstall the IMPAX Migration Tools from a Solaris computer

1. Log in as the **root** user.
2. Type **pkgrm IMPAXmigration**.
3. Type **y** to remove the package.
4. Type **y** again to continue removing the package.

   At the end of the removal process, the message `Removal of <IMPAXmigration> was successful` is displayed.

14. Uninstalling the Cross-Cluster Dictation Interlock tool

(Topic number: 60396)

If you no longer have to synchronize the dictation status of studies between the previous version and the 6.5.1 IMPAX systems, you can uninstall the components of the Cross-Cluster Dictation Interlock tool.

To uninstall the Cross-Cluster Dictation Interlock tool

1. On the previous version IMPAX Application Server where the Cross-Cluster Dictation Interlock components were installed, open the Windows Administrative Tools and select **Services**.
2. Right-click the **Impax Study Status Relay** service and select **Stop**.
3. Close the Services window by selecting **File** > **Exit**.
4. Open a command prompt.
5. Change to the directory containing the Cross-Cluster Dictation Interlock components—possibly C:\Program Files\Agfa\Impax Business Services.
6. Type **uninstall_study_status_relay_service.bat**.
7. Close the command prompt by typing **exit**.
8. From Windows Explorer, navigate to and delete the **study-status-signal-relay** folder (possibly from C:\Program Files\Agfa\Impax Business Services).
9. On the IMPAX 6.5.1 Application Server where the 6.5.1 Cross-Cluster Dictation Interlock components were copied, follow steps 1 to 7.
10. Log into a previous version IMPAX Client as an administrator user.
11. From the Configure area - Users and Roles section, delete the **remote-dictation** user from the Study Status Relay role, then delete the **Study Status Relay** role.
12. Log into an IMPAX 6.5.1 Client as an administrator user and repeat the previous step on it.

All components of the Cross-Cluster Dictation Interlock tool are now removed.

15. Updating Heartlab polling procedures

(Topic number: 60384)

If integrating with Heartlab software, after the upgrade is completed, enable procedures to poll for Heartlab updates.

To update Heartlab polling procedures

1. On the Database Server, log in as the **oracle** user.
2. Run the following script from sqlplus:

   update map_ini set ini_value = 'T' where ini_key = 'HEARTLAB_ENABLED';

An Oracle job is now created on the Heartlab database server to poll for updates every 5 minutes.

16. 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.

Oracle Data Guard: Disaster recovery solution

A

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 166).

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 144).

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 144). 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 144)

     or

   - Cold backup and restore (refer to page 148)

   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 155) 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 148). 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 145).
3. For Solaris servers only: Share the Flashback area (refer to page 146).

4. Run the Oracle Data Guard configuration on the standby server (refer to page 147).
5. Complete the Data Guard configuration on the primary server (refer to page 148).
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 (refer to page 146); otherwise go directly to restoring the database on the standby server (refer to page 147).

Sharing the Flashback Recovery Area and the primary /dbase partition on a Solaris Server

(Topic number: 125477)

Important!

This task is **not** required on Windows servers.

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

To share the primary Flashback Recovery Area and the primary /dbase partition on a Solaris server

1. Copy the contents of the Flashback directory from the primary to the standby server.
2. Open the file **/etc/dfs/dfstab** in a text editor.
3. Add the following line:

   share –F nfs -o rw,anon=0 *path_to_Flashback_recovery_area*

4. Save and close the file.
5. If the system is armored, type

   svcadm enable network/nfs/server

6. Type **shareall**.
7. Log in as the **mvf** user.

8. To confirm that the directory was shared, type **dfshares**.

Next, restore the database on the standby server (refer to page 147).

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 148).

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 155) 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 144) 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 149).
2. Start the public listener (refer to page 150).
3. Run the Oracle Data Guard configuration on the standby server (refer to page 150).
4. For Solaris servers only: Share the primary Flashback and database areas (refer to page 151).
5. Restore the database on the standby server (refer to page 151).
6. Complete the Data Guard configuration by linking the two servers (refer to page 154).

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 150).

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 (refer to page 151); otherwise, if using Windows servers, restore the database on the standby server (refer to page 151).

Sharing the primary Flashback Recovery Area and primary /dbase partition on a Solaris Server

(Topic number: 123990)

Important!

This task is **not** required on Windows servers or on the standby database server. It requires a root user login.

If the database volumes are mounted using NFS then this procedure must be completed from the NAS hosting the NFS share to the primary server.

To share the primary Flashback Recovery Area and primary /dbase partition on a Solaris server

1. Type **shareall**.
2. Open the file **/etc/dfs/dfstab** in a text editor.
3. Add the following line:

   share –F nfs -o rw,anon=0 *path_to_Flashback_recovery_area*

   share –F nfs -o rw,anon=0 /dbase
4. Save and close the file.
5. If the system is **not** armored, type **shareall**.

   or

   If the system is armored, type

   svcadm enable network/nfs/server

   shareall
6. Log in as the **mvf** user.
7. To confirm that the directory was shared, type **dfshares**

Next, restore the database on the standby server (refer to page 151).

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*	–
/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 154).

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 155) 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 164).

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 164).

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.

Script	Description
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;

Troubleshooting: Reducing the time needed for a Solaris client to connect to the Oracle standby server

(Topic number: 111472)

Issue

After Oracle Data Guard has failed over to the standby server, there is a long delay before Solaris clients such as Network Gateways can connect to the standby database. This delay can be up to 3 minutes long. During this time, IMPAX essentially ceases to function.

Details

The delay is caused by the TCP/IP settings. You can significantly reduce this time interval by changing the TCP/IP values on the Oracle database's Solaris clients.

Solution

Important!

This solution applies to Solaris servers only. This procedure is not necessary on Windows clients in a mixed-host cluster.

On each of the Oracle database's Solaris clients, change the TCP/IP values as follows:

1. Log in to one of the Oracle database's Solaris clients and open a command prompt.
2. View the current TCP settings by typing:

   ndd -get /dev/tcp tcp_ip_abort_cinterval

   ndd -get /dev/tcp tcp_ip_abort_interval

   ndd -get /dev/tcp tcp_keepalive_interval
3. Record these values in case you have to reset them.
4. Change the current TCP settings by typing:

   ndd -set /dev/tcp tcp_ip_abort_cinterval 10000

   ndd -set /dev/tcp tcp_ip_abort_interval 60000

   ndd -set /dev/tcp tcp_keepalive_interval 240000

After modifying the TCP/IP values, the client will connect to the standby Oracle database much faster than before.

Troubleshooting IMPAX B

As you upgrade IMPAX servers, you may encounter various problems.

Troubleshooting: Reports not displaying on the IMPAX Client—no default report source

(Topic number: 120765)

Issue

Reports are not displaying on the IMPAX Clients.

Details

After upgrading to IMPAX 6.5.1 from a version prior to IMPAX 6.3, IMPAX Clients cannot retrieve reports because no default report source is configured. This situation may arise even when a valid report source is specified during the upgrade process.

Solution

On the IMPAX Client, if a user opens a study and the expected report is not displayed, check the Application Server's AgfaHC.Pacs.Web.Services.Log file for error messages that indicate a default report source could not be found. If you find this type of message in the log file, configure a default report source.

1. Log into the Application Server.
2. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Configurator Tool**.
3. Switch to the **Web Services** tab.
4. If the Report Sources Info field contains entries, double-click one of the entries.

   or

If the Report Sources Info field is empty, click **Add**.

5. In the Report Source Provider field, type a name for the report source.
6. From the RIS type list, select the appropriate RIS type.
7. If you selected either Connectivity Manager Queryable RIS or Remote Agfa RIS in the previous step, in the URL field, enter the URL for the queryable RIS or the remote RIS.
8. If **Default Report Source** is not selected, select it.
9. To close the Edit Report Source dialog, click **OK**.
10. Click **Apply**. Click **OK**.

Troubleshooting: How do I manually upgrade individual Solaris servers?

(Topic number: 60646)

Issue

I need to manually upgrade an individual Solaris server; for example, after running the Trust Tool to upgrade all the Solaris servers in the cluster, testing reveals that one of the servers did not get upgraded.

Solution

You can manually upgrade individual Solaris servers by running the impax_install script.

To upgrade a Solaris server

1. To upgrade the Database Server, log into the Database Server as the **root** user.
2. To upgrade an AS3000 Network Gateway or Archive Server station, from the Database Server hosting the repository, log into the remote station as the **root** user.
3. Navigate to the IMPAX software repository location.
4. At the prompt, type

   ./impax_install upgrade
5. Respond appropriately to all prompts.
6. After the upgrade installation process is complete, type the following to clear volatile memory (RAM) to disk and reboot:

   sync ; sleep 10 ; init 6
7. Check the log file **/usr/mvf/data/logs/IMPAX_install.log** for any error messages.
8. Repeat this process for any other servers to be upgraded.

Troubleshooting: Database restores from disk are very slow

(Topic number: 60628)

Issue

Restoring the Oracle database from disk is extremely slow.

Details

When the disks containing the Oracle data files are mounted with the ForceDirectIO option, recovering an Oracle database from disk is extremely slow.

Solution

Perform the following procedure to mount the database without ForceDirectIO:

1. As user root, check to see whether the database is mounted with ForceDirectIO. At a terminal window, type:

   grep 'dbase' /etc/vfstab | grep 'forcedirectio'

   If this command does not return any output, the disks are not mounted with ForceDirectIO and are not the cause of the performance problem.

   But, if this command returns output similar to the following, the /dbase disks are mounted with the ForceDirectIO option:

   ```
   /dev/dsk/c2t5d0s7     /dev/rdsk/c2t5d0s7    /dbase/data1 ufs 2 yes
   forcedirectio
   /dev/dsk/c2t5d3s7     /dev/rdsk/c2t5d3s7   /dbase/index1 ufs 2 yes
   forcedirectio
   /dev/dsk/c2t5d1s7     /dev/rdsk/c2t5d1s7    /dbase/system ufs 2 yes
   forcedirectio
   dev/dsk/c2t5d2s7     /dev/rdsk/c2t5d2s7    /dbase/redo ufs 2 yes
   forcedirectio
   ```

2. Change directory to ensure that you are not in the /dbase directory.
3. To remount the /dbase disks without ForceDirectIO, type

   # mount -o remount,noforcedirectio /dbase/data1

4. Re-enable ForceDirectIO.

CAUTION!

Failure to re-enable ForceDirectIO negatively affects database performance.

Troubleshooting: Images intermittently not being displayed

(Topic number: 60411)

Issue

Periodically the impax.log file registers aspftp errors reporting `cannot decode ticket contents` and `key not found`.

Details

This problem can occur if the portable password is missing, or if the server clocks are not synchronized.

Solution

1. Import the portable password file from the Database Server onto all cached servers.
2. Confirm that clocks are synchronized (refer to page 140) between the Application Server and all cached servers.

Troubleshooting: Cannot reboot with the init 6 command

(Topic number: 6897)

Issue

When the **impax_install upgrade** finishes, you are prompted to reboot the machine by running **init 6**. This command does not reboot the machine; it appears to hang during shutdown.

Details

This problem is caused by a process stuck in a low level i/o request waiting for the kernel to receive an interrupt or dma transfer to complete. The kernel puts a process on a channel wait queue, waiting for an interrupt until the i/o is complete. If a disk never completes an i/o due to a hardware error, it does not go on the run queue to service the interrupt and become killable.

This state can be invoked by:

- Direct-attached disk or disk cabling errors causing an i/o to not complete.
- NFS synchronous i/o, where the network connection has failed.
- The console i/o and the master console (which may be typically a physical console or serial port) being disconnected. Console i/o is always direct and synchronous for security reasons and the lack of console i/o causes auditing problems.

Solution

Contact your Agfa HealthCare Support representative for assistance.

Troubleshooting: Oracle Server upgrade fails due to mounted repository

(Topic number: 68114)

Issue

After mounting the Oracle software repository, the Oracle Server upgrade script (upgrade-oracle or upgrade-oracle-dg) fails with the following error:

```
Error: /tmp/Oracle10.2.0.1.0/runInstaller exited with an error, exiting.
Error: Oracle installion (sic) failed, exiting.
There were problems installing Oracle Server. Please correct any problems
before re-running this script.
```

Details

The upgrade script fails if the mounted repository is not unmounted prior to running the script.

Solution

Refer to the following lines in the /var/sadm/Oracle_install.log file:

```
Error: OUI cannot be launched because the current working directory is set on
 the CD-ROM mount point.
Launching OUI from this directory will make it difficult to unmount the disk
later in the installation.
Please change the working directory and relaunch OUI. You can change the working
 directory by typing 'cd' (e.g. cd /home) and then execute the 'runInstaller'
 command by typing its full path (e.g. /mnt/cdrom/runInstaller)
Error: /tmp/Oracle10.2.0.1.0/runInstaller exited with an error, exiting.
Error: Oracle installion (sic) failed, exiting.
```

Troubleshooting: This is not a Data Guard configuration error message

(Topic number: 99770)

Issue

After running the upgrade-oracle-dg script which upgrades an Oracle Data Guard server, it fails with the following error:

```
This is not a Data Guard configuration. Please run upgrade-oracle instead.
```

Details

The message may be misleading; the upgrade script fails if Oracle has not been started on the primary and all standby Data Guard servers.

Solution

Ensure that Oracle has been started on the primary as well as all standby Data Guard servers.

Troubleshooting: After upgrading and rebooting, Oracle fails to start

(Topic number: 6907)

Issue

After running the impax_install upgrade script and rebooting, Oracle fails to start.

Details

This failure occurs when no semaphore allocation settings appear in /etc/system.

Solution

As user **root**, check for the following lines in the /etc/system file. If they do not exist, add them to the file and reboot.

```
*** Begin Oracle requirements ***
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
set shmsys:shminfo_shmmin=1
set semsys:seminfo_semmni=100
set semsys:seminfo_semmns=2048
set semsys:seminfo_semmsl=256
set semsys:seminfo_semvmx=32767
set noexec_user_stack=1
*** End Oracle requirements ***
```

Troubleshooting: IMPAXarmr entries are missing after upgrading

(Topic number: 6879)

Issue

After running the impax_install upgrade script, IMPAXarmr entries are missing from the /etc/system file.

Details

The missing IMPAXarmr entries occur after upgrading to IMPAX 6.5.1 from a site that does not already have armoring installed. As a result, auditing information is not tracked. This does not affect machine security itself, but attempts to exploit the stack buffer overflow are not logged. This occurs only on the Database Server, and only when using Solaris 9. More information is available in *Understanding Solaris armoring* (refer to page 184).

Solution

The workaround is to add the following lines to the /etc/system file, as user root, before rebooting:

```
*** Begin IMPAXarmr modifications ***
set noexec_user_stack=1
set noexec_user_stack_log=1
*** End IMPAXarmr modifications ***
```

Troubleshooting: IMPAX Client slow and erratic post-upgrade

(Topic number: 10210)

Issue

After upgrading, IMPAX Client display is very slow at a site using McAfee Antivirus software.

Details

A McAfee Antivirus setting called Buffer Overflow Protection (BOP) can cause this behavior.

Solution

Disable BOP in McAfee. Alternatively, use McAfee EPO or Protection Pilot to reconfigure the BOP to run only at fixed intervals, such as every five minutes.

Troubleshooting: Import of portable password file failed during upgrade

(Topic number: 61095)

Issue

The portable password file was not available on the Database Server when the AS3000 Archive Server or Network Gateway was installed, so the AgfaService ID password file failed to import properly on these servers.

Details

Whenever the import of mvf.portable.psd to the target server fails during an installation, you see the following log message indicating that 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.
```

Solution

The Network Gateway or Archive Server upgrade completed successfully (unless other log messages indicate otherwise), but you must manually import the password key to the target server. Instructions on generating the portable password file are available in *Generating the portable password file* (refer to page 80).

To import the portable password file locally to the target server

1. Log into the target Network Gateway or Archive Server as **root**.
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, delete the portable password file from all locations after all required components are installed.

Troubleshooting: Application Server installation error

(Topic number: 96652)

Issue

When upgrading the Application Server, the following error appears:

```
Product: AGFA IMPAX Business Services -- Error 1335.The cabinet file 'Data1.cab'
required for this installation is corrupt and cannot be used. This could indicate
a network error, an error reading from the CD-ROM, or a problem with this package.
```

Details

Data1.cab files are left over from previous installations of the Application Server and cause problems with the InstallShield.

Solution

Delete all the Data1.cab files in the temp folder (%TEMP%).

Troubleshooting: Must back out of the Application Server upgrade

(Topic number: 60757)

Issue

A problem has occurred and I must return to the previous version of the Application Server software.

Solution

To back out of the Application Server upgrade

1. Back up the web.config files and note the location of the current web.config files.
2. On the Application Server, open Control Panel.
3. Select **Add or Remove Programs**.
4. Remove **AGFA IMPAX Business Services** and **IMPAX Installation Server**.

   Do not remove ADAM (Windows 2003) or AD LDS (Windows 2008).
5. Install the previous version (IMPAX 6.2 or later) of the Server, Application Server, and Client Installation Server software.

Note:

By installing an earlier version of the Client Installation Server, the Client workstation software is automatically rolled back within an hour for online workstations.

Troubleshooting: How do I determine which users are ADAM administrators?

(Topic number: 60661)

Issue

How do I determine which users are ADAM administrators?

Solution

If the site uses other dedicated Application Servers, you can determine which users on the Application Servers are ADAM administrators:

1. On an Application Server, select **Start** > **All Programs** > **ADAM** > **ADAM ADSI Edit**.
2. Select **Well-known naming context** and select **Configuration** from the list.
3. Click **OK**.

   If this step fails, you are not logged into the Application Server as an ADAM administrator. Log in as the user who originally installed ADAM or who has been added as an ADAM administrator and try these steps again.
4. Expand the new Configuration node and select **CN=Configuration** > **CN=Roles**.
5. Double-click **CN=Administrators**.
6. Double-click the **member** attribute.

   The ADAM administrators are listed by login name.

Troubleshooting: How do I determine which ADAM instance is the Schema Master?

(Topic number: 60664)

Issue

How do I determine which ADAM instance is the Schema Master?

Solution

If the site uses other dedicated Application Servers, you can determine which one is running the master ADAM instance to find out which is the Schema Master:

1. Select **Start** > **Run** and type **mmc**.
2. In the Console dialog, select **File** > **Add/Remove Snap-in**.
3. In the Add/Remove Snap-in dialog, click **Add**.
4. From the Snap-in list, select **ADAM Schema** and click **Add**.
5. To close the Add Standalone Snap-in dialog, click **Close**.
6. To close the Add/Remove Snap-in dialog, click **OK**.
7. Right-click ADAM Schema and select **Change ADAM Server**.
8. In the Connect to ADAM Server dialog, enter localhost as the ADAM server and add the port, usually 389.
9. Select This Account and select a user that is an ADAM Administrator from the list.
10. Click **OK**.
11. Right-click ADAM Schema and select **Operations Master**.

The current Schema Master is listed in the dialog. This is the Application Server on which to upgrade the ADAM database.

Cache check tools reference

C

IMPAX 6.5.1 includes four tools designed to ensure the integrity of the IMPAX cache directory. These tools check the cache directory, repair the cache directory, and then provide a 'Loss Report' for files missing from the cache.

mvf-check-cache

(Topic number: 60503)

This command checks that all the DICOM object files registered in the database for a particular cache volume actually exists in the cache. It also does a sanity check to determine whether the files are correct by comparing the sop_instance_uid to the value in the database. A report giving precise details of the problems found is produced and written to the log file. Optionally, a move-cmds.sh file is created to move the problematic files out of the cache. Files in the cache that do not have locations registered in the database are not detected by mvf-check-cache.

If there are multiple caches, the path name of the cache to be checked must be specified. Memory usage may be high if there are a large number of files, but mvf-check-cache displays the amount of memory required so that the operator can add more virtual memory if needed

Performance of mvf-check-cache is hardware dependant. For example, on a Sunfire 280R, mvf-check-cache can check about 130 files per second. With the quick check option enabled (checking only file existence and file size), about 30,000 files per second can be checked.

mvf-clean-cache

(Topic number: 60506)

This command scans an IMPAX cache directory containing DICOM object files and generates a report of files that do not belong there, either because the file name format is invalid or because this location for the object file is not registered in the database. While working, it writes messages to the

stderr stream to keep the tool operator informed of its progress. The path name of the cache to be scanned is specified on the command line. mvf-clean-cache begins by querying the database for the list of ordinals for the files in the cache. It keeps this list in memory. If there is a large number of files, memory usage may be high but mvf-clean-cache displays the amount of memory required and the operator can add more virtual memory if necessary.

mvf-clean-cache does not access the contents of the cache files. It works by examining the file names and reporting the problem. A copy of the report and additional diagnostic messages are written to the log file. Since mvf-clean-cache may be run on a live system, new files (less than one hour old) are skipped. Thus, temporary files created by the SCP are ignored.

Performance of mvf-clean-cache is hardware dependent. For comparison, on a Sunfire 280R, mvf-clean-cache can check approximately 50,000 files per second

mvf-ddo-rescue

(Topic number: 60521)

This command takes any number of files and directory arguments to determine whether they are DICOM objects. If the argument is a directory, it analyzes all the files in that directory and recursively analyzes all files in all subdirectories. If a file is a DICOM object, then mvf-ddo-rescue determines whether the DICOM object is damaged. If it is undamaged, then mvf-ddo-rescue attempts to find the object in the database. If the object is found in the database, mvf-ddo-rescue checks for a local cache location for the object. If a local cache location is found, then mvf-ddo-rescue compares the DICOM object file with the DICOM object file in the cache to see whether:

1. The cache file is missing
2. The cache file is a duplicate

   or
3. The cache file is different

If a problem exists, mvf-ddo-rescue attempts to give precise details. A copy of the report and additional diagnostic messages are written to the log file.

Performance of mvf-ddo-rescue is hardware dependent. For example, on a Sunfire 280R, mvf-ddo-rescue can analyze about 40 files per second. Performance also depends on how many files must be identified by searching the original_sop_instance_uid field in the database.

mvf-report-loss

(Topic number: 60524)

After repairs have been performed by mvf-check-cache (refer to page 181) mvf-clean-cache (refer to page 181), and mvf-ddo-rescue (refer to page 182), mvf-report-loss is used to perform the last two steps of the repair process:

1. It determines what cache files have been lost and generates a "Loss Report" for the customer. The body of the report contains one line for each study affected and the report is sorted by patient name and study date.

2. It unregisters the missing cache files from the database, preventing display, transmit, and archive errors that are caused when the product tries to access files that are missing from the cache.

mvf-report-loss has two corresponding modes of operation:

Marking mode

The default mode for the tool. In marking mode, the tool checks all the caches on the local server for the presence of the DICOM object files that the database says should be present. For missing files, the "visible" field in the database osr_location table is set to 'C'. (Normally this field contains the value 'T' for true, or 'F' for false). Changing this field makes these file locations invisible to the product software.

The reporting tool may be rerun after further recovery work has been completed (more files restored to cache). In these cases the tool also checks locations with visible value 'C'. If any files have been restored to cache since the last run of the tool, it sets those locations' visible values back to 'T' to indicate that they are now valid.

After the missing DICOM object file locations are marked, a report is generated for the studies that contain lost objects. Each comma-delimited line in the report lists the patient name, patient ID, modality, accession number, study description, study date, total number of objects, and number of lost objects for an affected study.

Note:

In the report, any commas in these fields are replaced by a semicolon.

Deregister mode (-r)

In deregister mode, the tool changes the 'C' values to 'F'. This triggers the Autopilot program to permanently delete these locations from the database. (This is a normal Autopilot function). Please note that there is **no undo**.

Note:

Before running the tool in deregister mode, check the report to ensure that the losses are as expected. If the report seems to report any files that may not be missing, follow the instructions given in the TROUBLE section. A copy of the report and additional diagnostic messages are written to the log file.

Performance of mvf-report-loss is hardware dependent. For comparison, on a standalone Sunfire 280R, mvf-report-loss scans about 2,000 files per second.

Security and licenses reference

D

Understanding security and license issues helps in completing the upgrade process.

Understanding Solaris armoring

(Topic number: 6915)

Solaris armoring disables non-essential system services and modifies system parameters to improve the security of the system. Solaris armoring is installed automatically as part of the Solaris 10 installation.

For systems that must connect to an external Network File System (NFS), such as Netapp Hierarchical Storage Management (HSM), the nfs.client must be re-enabled and started on all systems that mount the NFS storage subsystem. This must be done after armoring is installed by typing the following:

svcadm -v enable -r network/nfs/client

svcadm -v restart svc:/network/nfs/client:default

Modifications made automatically by the Solaris armoring installation

(Topic number: 6954)

Solaris armoring installation makes the following modifications to a standard Solaris install:

- Removes all unnecessary services from /etc/inetd.conf.
- Disables ftp, telnet rsh access (to be replaced by scp and ssh).
- Turns off a number of unnecessary services in the rc scripts.
- Locks down .rhosts, .netrc, and hosts.equiv files (rsh no longer functions, replaced by ssh).

- Enables sulogging, tcpdlogging, inetlogging, and login log, which improve the system's IDS capabilities.
- Modifies the /etc/default/inetinit sets TCP_STRONG_ISS = 2.
- Randomizes all initial sequence number for all TCP connections, guarding against IP spoofing and hijacking.
- Secures the kernel parameters for /dev/ip by restricting IP querying.
- Modifies /etc/system to help protect against buffer overflow attacks.

Groups and accounts created for IMPAX

(Topic number: 6976)

Certain operating system groups and accounts are created for IMPAX when it is installed.

Operating system groups created for IMPAX

During the IMPAX installation, the following operating system groups are created:

Group	Description
dba	Group created for database activities
mitra	Created for IMPAX activities

Operating system account created for IMPAX

During the IMPAX installation, the following operating system account is created, with a secure password:

Account	Description
mvf	Account for administrative IMPAX access

Accounts created for IMPAX

Account	Description
oracle	Administrator account for the Oracle database, with a secure password
ocr_train	User account created when optional MVFocr package is 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.

Cygwin

(Topic number: 121758)

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

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

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

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

Preamble

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

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

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

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

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

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

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

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

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

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

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

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

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

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

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

      The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all

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

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

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

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

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

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

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

END OF TERMS AND CONDITIONS

Editline 1.2-cstr

(Topic number: 121768)

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

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

APIP

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

Autopilot

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

B

browser

Software that allows a user to search through information on a server. The term usually refers to a universal client application, such as Firefox or MS Internet Explorer, that interprets HTML documents.

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.

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.

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.

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.

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.

HTTPS

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

L

log file

A file or set of files containing a record of the actions and modifications made in an application. Service teams use log files during setup and configuration of the system or its components. Logs are also used to diagnose problems. Logging can typically be set to record varying levels of detail.

M

master Curator

When using multiple Curators, the first Curator that runs, which owns the job queue.

modality

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

N

NAS

Network Attached Storage. A storage device attached directly to a Storage Area Network (SAN) or other direct network connection.

network

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

Network Gateway

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

O

OCR

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

P

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.

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.

scheduled worklist

A worklist that you can set to occur on specific days, that holds the studies for a round, clinic, or conference. You can prepare for a round by taking snapshots of study layouts with the Snapshot tool and saving the snapshots in a scheduled worklist.

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.

W

warm backup

Descriptive of a backup process in which the database does not have to be shut down. Compared with cold backups, warm backups are faster and keep the database accessible while the backup is being performed.

wizard

Wizards are used to automate processes. Wizards perform a predetermined sequence of actions after they are selected and applied.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z