AS300 Upgrade and Migration Guide

IMPAX 5.2 or 5.3 to IMPAX 6.5.1

Migrating the Components of an IMPAX 5.2 or 5.3 AS300 Cluster to IMPAX 6.5.1

AGFA

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 140).

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

1 Getting started 9

Valid IMPAX upgrade paths....9
Related documentation: IMPAX upgrades....10
IMPAX hardware and software requirements....11
IMPAX Application Server hardware and software requirements....11
IMPAX AS300 Server hardware and software requirements....13
Curator hardware and software requirements....16
IMPAX Client hardware and software requirements....18
System requirements for upgrading standalone stations....20

2 Preparing to upgrade 22

Gathering information and equipment....22
IMPAX 5.2 or 5.3 upgrades: Necessary information and equipment....22
Running the Cross-Cluster Dictation Interlock tool....23
Taking a system snapshot....24
Emptying Connectivity Manager queues....24
Stopping Connectivity Manager interfaces....25
Stopping Connectivity Manager queues....25
Stop transmitting data to IMPAX....26
Redirecting studies to the training server....27
Archiving remaining unarchived studies....27
Verifying unverified studies....27
Storing unarchived studies....28
Closing and mirroring archive volumes....28
Emptying all queues....29
Halting all queues....29
Deleting cache locations for studies....30
Stopping antivirus software....31
Clearing the archive Logical Volume....31
Deleting old log files....32
Uninstalling IMPAX documentation....32
Uninstalling IMPAX 5.2 or 5.3 documentation....32

3 Upgrading and configuring external software 34

Upgrading Windows 2003 to Windows 2008....34
Upgrading to Windows Server 2008....34
Configuring Windows 2008....35
Upgrading Windows Server 2008 to Windows Server 2008 SP2....35
Enabling Automatic Updates for Windows....36
Enabling Automatic Updates for critical Windows XP or 2003 updates....36
Enabling Automatic Updates in Windows 2008....37
Upgrading to Internet Explorer 7....37
Enabling active content for the Knowledge Base....38
Enabling remote access to Knowledge Bases....38
Enabling local access to Knowledge Bases....39

4 Upgrading an existing Database Server to IMPAX 6.5.1 40

Upgrading SQL Server database software....40
Upgrading SQL Server 2000 to SQL Server 2008....40
Stopping SQL Server 2008 services....43
Upgrading SQL Server 2008 to SQL Server 2008 SP1....43
Upgrading the IMPAX 5.2 or 5.3 database schema to IMPAX 6.5.1....44
Checking the status of SQL Server upgrades....45
Migrating data from the training server....46
Taking the training server offline....46
Backing up the training server database....47
Migrating worklist and report data....47
Uninstalling the previous IMPAX software packages....49
Determining a password for the AgfaService account....50
32-bit AS300 installer packages reference....50
AS300 installer log files....53
Upgrading the IMPAX AS300 32-bit Database Server software....53
Generating the AS300 portable password file....56
Updating the SQL Server registration....57
Configuring Data Execution Prevention (DEP)....57

5 Replacing an existing Database Server with a new station 59

Backing up the AS300 SQL 2000 database....59
Installing the 32-bit IMPAX 6.5.1 AS300 packages on a new Database Server....60
Restoring the upgraded database on a new Database Server....61
Upgrading the IMPAX 5.2 or 5.3 database schema to IMPAX 6.5.1....63
Checking the status of SQL Server upgrades....64
Migrating data from the training server....65
Taking the training server offline....65
Backing up the training server database....66
Migrating worklist and report data....66
Installing Oracle 10.2.0.1 OLE drivers on the Application Server....68
Generating the AS300 portable password file....69

6 Upgrading other AS300 servers to IMPAX 6.5.1 70

Uninstalling the previous IMPAX software packages....70

Configuring the ODBC connection to the SQL Database Server....71
Installing the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages....72
Installing and configuring Store and Remember archiving....75
Configuring Data Execution Prevention (DEP)....75

7 Reconfiguring the Application Server and Curator 77

Reconfiguring the Application Server....77
Disabling SQL connections....78
Connecting to the IMPAX 6.5.1 SQL Server database....78
Importing the portable password file to the Application Server....80
Setting the password and account lockout policies....80
Connecting the Application Server to a non-queryable non-IMPAX RIS....80
Performing other Application Server configurations....81
Reconfiguring the Curator....82
Uninstalling IMPAX 6.5.1 Server....82
Uninstalling Oracle on Windows....83
Installing and configuring the Oracle 10g Client for Windows....84
Configuring the ODBC connection to the SQL Database Server....85
Setting up the Curator web cache....86
Preparing the web cache....88
Performing other Curator configurations....89

8 Completing the upgrade and migration 90

Migrating a cache volume from a flat to a hierarchical structure....90
Configuring the Audit Record Repository database connection....92
Changing the SQL Server administrator (sa) password....93
Synchronizing clocks on Windows-based IMPAX systems....94
Synchronizing Windows servers to an external time source....94
Synchronizing Windows servers to an internal time source....95
Synchronizing with a time server when the IMPAX computer is not a member of a domain....96
Synchronizing with a time server when the IMPAX computer is a member of a domain.96
Upgrading Clients to IMPAX 6.5.1....97
Manually uninstalling the IMPAX 5.2 or 5.3 Client software....97
Removing the IMPAX 5.2 or 5.3 Client Knowledge Base....98
Installing the IMPAX Client....98
Restarting antivirus software....100

9 Post-upgrade checking and stabilization 101

Installing Server license keys on an upgraded AS300 server....101
Installing the mvf license key on a Windows server....101
Installing the archive license key on a Windows server....102
Testing the installed software....102
Restarting an archive queue....103
Restarting Connectivity Manager queues....104
Taking a post-upgrade system snapshot....104
Comparing pre- and post-upgrade snapshots....105

Installing the PSARMT and cache tools on a Windows server....105
Running PSARMT to mark studies from an external PACS as PACS archived....106
Uninstalling the IMPAX Migration Tools from a Windows computer....107
Uninstalling the Cross-Cluster Dictation Interlock tool....107
Stopping WEB1000 Data Currency service....108
Stopping the exhibitSyncNotifier service....109
Uninstalling Data Currency from an AS300 server....109
Removing Client queues from Job Manager....110

Appendix A: Configuring Oracle Data Guard 111

Oracle Data Guard configuration overview....111
Installing the Oracle Data Guard package on a Database Server....112
Configuring Oracle Data Guard using RMAN....112
Running the Oracle Data Guard configuration on the primary server....113
Restoring the database on the standby server....114
Completing the Data Guard configuration....115
Configuring Oracle Data Guard using cold backup....116
Running the Oracle Data Guard configuration on the primary server....117
Running the Oracle Data Guard configuration on the standby server....118
Sharing the primary Flashback Recovery Area and primary /dbase partition on a Solaris Server....119
Restoring the database on the standby server....119
Completing the Data Guard configuration....122
Configuring RMAN backups after the Oracle Data Guard configuration....123

Appendix B: Troubleshooting IMPAX 125

Troubleshooting: “Finding uninstall information for the previous version of Impax” error during AS300 upgrade....125
Troubleshooting: When upgrading an AS300 to IMPAX 6.5.1, the Cygwin installation hangs.126
Troubleshooting: Reports not displaying on the IMPAX Client—no default report source....128
Troubleshooting: Some sites may notice a delay in updating clusters....129
Troubleshooting: IMPAX Client slow and erratic post-upgrade....129
Troubleshooting: Reports not displaying on the IMPAX client....130
Troubleshooting: Unlocking the mvf user account....131
Troubleshooting: Server name registered in SQL Server is incorrect....132

Appendix C: Cache check tools reference 133

mvf-check-cache....133
mvf-clean-cache....133
mvf-ddo-rescue....134
mvf-report-loss....134

Appendix D: IMPAX 5.2 tables obsolete in IMPAX 6.5.1 136

Obsolete tables in WSQL....136
Obsolete tables in ORAS....138

Appendix E: External software licenses 140

AutoFac 2.1.13....140
Cygwin....141
Editline 1.2-cstr....146
ICU License - ICU 1.8.1 and later....146
OpenSSL....147
Xerces C++ Parser, version 1.2....149
Zlib....149

Glossary....150

Index....154

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 5.2 or 5.3 cluster to IMPAX 6.5.1. It is a companion volume to the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 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

Component	Requirements
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

Component	Requirements
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	StorageTek (STK)	D series

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

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

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 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)

Component	Requirements
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) 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 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

Component	Requirements	
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 PCle for Coronis BarcoMed PCle for Nio BarcoMed PCle 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 ATI 3700, 3750, V3800 (third monitor board) MXRT 1150/2150 (third monitor board)	**Windows XP and Vista:** NVIDIA FX 1700, FX 1800, FX 4800 ATI 3700, 3750, V3800 (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.

System requirements for upgrading standalone stations

(Topic number: 114785)

Existing IMPAX standalone stations can be upgraded to IMPAX 6.5.1:

- If they are on IMPAX 6.5 and running on Windows 7 (host operating system) and Windows Server 2008 (guest operating system) using VMware Player.

  or

- If they are currently running on Windows XP and if they meet the minimum hardware requirements. If running SQL Server 2000, an upgrade to SQL Server 2008 is required. (If running SQL Server 2005, this version can be retained.)

Follow the procedures in the *IMPAX 6.5.1 Standalone Upgrade Guide*.

Stations that do not meet the minimum hardware requirements or that require an operating system upgrade cannot be upgraded. Instead, a new standalone installation must be performed, following the procedures in the *IMPAX 6.5.1 Standalone Installation and Configuration Guide*.

Component	Minimum hardware requirement for standalone upgrade
Workstation	HP xs6600 or equivalent
RAM	4 GB
CPU	1 x Dual-Core (Intel XEON 52xx)
Video	For enhanced CT/MR navigation, minimum BARCO MXRT-5200

Preparing to upgrade

2

Important!

Before proceeding with the upgrade of the AS300 server components, ensure that you have completed the tasks outlined in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

You must perform certain preparatory tasks before upgrading to an IMPAX 6.5.1 AS300 configuration. These tasks include taking a system snapshot, stopping the transmission of data to the previous release of IMPAX, and emptying and halting queues.

1. Gathering information and equipment

(Topic number: 10190)

To perform the AS300 server upgrade and migration, gather the information and equipment needed for migrating and upgrading the stations.

IMPAX 5.2 or 5.3 upgrades: Necessary information and equipment

(Topic number: 10231)

Equipment and information for upgrading existing IMPAX 5.2 or 5.3 stations	Notes
Whether to upgrade to Microsoft Windows Server 2008 Server SP2. If sticking with Windows 2003, you must obtain Microsoft Windows Server 2003 R2 SP2. If upgrading to Windows Server 2008 Server SP2, you must acquire that software.	

Equipment and information for upgrading existing IMPAX 5.2 or 5.3 stations	Notes
Whether Cross-Cluster Dictation is required, for synchronizing dictation status between IMPAX 5.2 or 5.3 and IMPAX 6.5.1.	
Whether to upgrade to SQL Server 2005 SP3 or switch to Oracle for Windows. If sticking with SQL Server, you must obtain the SQL Server 2008 software and service pack. If switching to Oracle for Windows, contact Agfa Professional Services for assistance. This guide does **not** document how to migrate from SQL Server to Oracle.	
Which standard time server or source to synchronize the server clock against.	
Whether using domain authentication.	
Whether worklists have been configured on the training server.	
Whether report data has been moved to the training server.	
Fully qualified domain name of the main Application Server.	
Whether any WEB1000 connections need to be managed.	
Whether to install a Curator or a CD Export server. If so, whether it is to be a dedicated Curator / CD Export server. If so, whether also installing slave Curators.	
Whether an Audit Record Repository is being added to the cluster.	

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 system snapshot

(Topic number: 7613)

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 that has access to the AS300 database to be migrated and on which the Migration Tools have been installed.

To take a system snapshot

1. At a command prompt, change to the **C:\mvf-mig6\bin** directory.
2. Type

   migration_inventory -d *database_name* -U *database_user_name* -P *database_password* -s -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, type

   mig_reporter -t system_inventory_tool

   This command writes the output of the migration_inventory command to a report file in the C:\mvf-mig6\reports directory. For other parameters you can use with the mig_reporter.exe command, refer to "mig_reporter.exe" (topic number 10619) in the appropriate version of the *IMPAX Preparing to Upgrade Guide*.

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. Stop transmitting data to IMPAX

(Topic number: 7617)

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

To stop transmitting data to IMPAX

1. Open the Windows Administrative Tools and select **Services**.
2. Right-click the **DICOM Service Class Provider** service and select **Properties**.
3. To change the Service status, click **Stop**.
4. From the Startup type list, select **Disabled**.
5. To close the Properties dialog, click **OK**.
6. Launch the IMPAX Service Tools and log in as user **service**.
7. On the Daily tab, select **Job Manager**.
8. Monitor each **Transmit** queue and wait for all outgoing jobs to finish.

   You cannot delete jobs in progress.
9. Select each Transmit queue and click **Halt Queue**. 
10. To confirm that you want to halt the queue, click **Yes**.

8. Redirecting studies to the training server

(Topic number: 10235)

Configure modalities to redirect studies to the training server system, so that they remain accessible to the IMPAX 6.5.1 Clients while the migration continues.

The details of how to redirect studies are modality-specific and are not covered in this guide.

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: 58295)

Before archiving studies, verify all unverified studies.

To verify unverified studies

1. In the Service 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 Service 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 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

10. Closing and mirroring archive volumes

(Topic number: 7733)

Close all open primary volumes before upgrading. Open mirror volumes are closed automatically when a SYNC job completes successfully with the corresponding closed primary volume. Fresh volumes may remain open as they do not contain any studies.

To close and mirror archive volumes

1. In the Service Tools, on the Setup tab, select **Archive Manager**.
2. Switch to the **Volumes** tab.
3. Select a logical volume and click **Close Logical Volume**.

4. If the system has a jukebox archive, you may have to wait for the sync job to finish.

   If the system has a non-jukebox archive, to ensure that a backup of the data exist, perform a mirror procedure manually.

5. On the Daily tab, select **Job Manager**.

6. Check the Delivery Date Time column for jobs that are not scheduled to run until later. If any exist, schedule these jobs to complete now, using the **Set Delivery Date and Time** option at the top.

11. Emptying all queues

(Topic number: 7702)

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

To empty all queues

1. In the Service Tools, on the Daily tab, select **Job Manager**.

2. If an archive job remains in any of the queues, select the job and click **Expedite Selected Job(s)**.

3. If any other job remains in any of the queues, select the job and click **Delete selected job(s)**.

12. Halting all queues

(Topic number: 59660)

Halt all queues until the upgrade is done.

To halt all queues

1. In the Administration Tools, on the Daily tab, select **Job Manager**.

2. In the queue list, select **All Queues**.

3. Click **Halt Queue**. 

4. To confirm that you want to halt the queues, click **Yes**.

13. Deleting cache locations for studies

(Topic number: 7707)

If you are replacing the 5.2 or 5.3 servers and are not restoring the files in the cache directory after the upgrade, to prevent database inconsistencies, remove all database references to images in cache. You must also do this for studies in Client caches, because IMPAX 6.5.1 no longer supports cached Clients—only cacheless and standalone Clients.

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

Note:

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

To delete cache locations for studies

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

   cache query

   A list of caches and their volume_refs is displayed.

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

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

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

3. To enter menu mode, type

   Go menu

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

   All studies in the volume_ref's cache are removed.

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

14. 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.

15. Clearing the archive Logical Volume

(Topic number: 7734)

Important!

This topic applies only when upgrading an existing server.

To avoid conflicts when upgrading, clear the archive Logical Volume. IMPAX re-creates the Logical Volume folders and files afterward.

CAUTION!

Ensure that the Logical Volume is empty before deleting it. If it is not empty, create a store job to archive the images in the Logical Volume.

To clear the archive Logical Volume

1. In the Service Tools, on the Setup tab, select **Archive Manager**.
2. Select the Logical Volume and click **Close**.
3. At the Close Volume prompt, click **Yes**.
4. Ensure that the Archive queue is halted.
5. Delete the Logical Volume folder and files from the drive.

The Logical Volume folder and files are automatically re-created by IMPAX.

16. Deleting old log files

(Topic number: 7706)

Important!

This topic applies only when upgrading an existing server.

On the server being upgraded, remove any old log files to ensure that all future log information is a result of the upgrade procedure.

To delete old log files

1. On the server to be upgraded, open a command prompt.
2. Change to the **C:\mvf\bin** directory.
3. Run **stopall.bat**.
4. For future reference, copy all files in C:\mvf\data\logs\ to a backup location.
5. Delete all the log files from C:\mvf\data\logs.

Important!

If you are running Oracle on Windows, do not delete the C:\mvf\data\logs\oracle directory.

17. Uninstalling IMPAX documentation

(Topic number: 7610)

You must uninstall any existing IMPAX documentation before you can install the new IMPAX 6.5.1 documentation.

Uninstalling IMPAX 5.2 or 5.3 documentation

(Topic number: 10734)

IMPAX 5.2 and 5.3 had separate Client and Server Knowledge Bases, each of which must be separately uninstalled. This documentation may have been installed on any 5.2 or 5.3 IMPAX Client or Server machines.

Removing the IMPAX 5.2 or 5.3 Client Knowledge Base

(Topic number: 58578)

If the IMPAX 5.2 or 5.3 Client Knowledge Base is installed, you must uninstall it before upgrading.

To remove the IMPAX 5.2 or 5.3 Client Knowledge Base

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

   or

   On Windows 2008 servers, click **Programs and Features**.
3. On Windows 2003 servers, select **IMPAX Client Knowledge Base 5.2** or **IMPAX Client Knowledge Base 5.3** and click **Change/Remove**.

   or

   On Windows 2008 servers, select **IMPAX Client Knowledge Base 5.2** or **IMPAX Client Knowledge Base 5.3** and click **Uninstall**.
4. In the Confirmation dialog, click **OK**.
5. If also uninstalling the IMPAX Server Knowledge Base, in the Maintenance Complete dialog, select **No, I will restart my computer later**. Otherwise, select **Yes, I want to restart my computer now** and click **Finish**.
6. If you restarted the computer, log into Windows as an administrator-level user.
7. To remove any translations of the IMPAX 5.2 or 5.3 Client Knowledge Base, delete the **C:/impax/documents/client/translations** directory.

Removing the IMPAX 5.2 Server Knowledge Base

(Topic number: 58581)

The IMPAX 5.2 Server Knowledge was used for both IMPAX 5.2 and 5.3 releases. If it is installed, uninstall it before upgrading.

To remove the IMPAX 5.2 Server Knowledge Base

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 Server Knowledge Base 5.2**.
4. On Windows 2003 servers, click **Change/Remove**. On Windows 2008 servers, click **Uninstall**.
5. In the Confirmation dialog, click **OK**.
6. In the Maintenance Complete dialog, select **Yes, I want to restart my computer now** and click **Finish**.

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

Upgrading and configuring external software

3

You may have to upgrade the operating system and database software on the server to meet IMPAX 6.5.1 requirements.

If staging new server computers rather than upgrading existing servers, you can skip these tasks and proceed with the *Replacing an existing Database Server with a new station* (refer to page 59) tasks.

1. Upgrading Windows 2003 to Windows 2008

(Topic number: 101638)

Microsoft recommends doing a clean installation of operating systems whenever possible. However if upgrading the operating system on an existing server is required, follow the instructions provided by Microsoft:

http://support.microsoft.com/kb/948070

2. Upgrading to Windows Server 2008

(Topic number: 7600)

IMPAX 5.2 and 5.3 can be run on the Microsoft Windows 2000 or Windows Server 2003 operating systems. When upgrading to IMPAX 6.5.1, you have the option of staying with Windows Server 2003 or upgrading to Windows Server 2008. If you are currently running Windows 2000, you must upgrade to Windows Server 2008. You cannot stay on Windows 2000.

Microsoft recommends doing a clean installation of operating systems whenever possible.

For detailed information regarding migration or upgrade to Windows Server 2008:

http://technet.microsoft.com/en-us/library/cc755199(WS.10).aspx

For information regarding Windows 2000 End-of-Support:

http://support.microsoft.com/ph/1131#tab0

Configuring Windows 2008

(Topic number: 109407)

After upgrading, configure Windows 2008 as follows:

- Activate Windows
- Set the Start menu and Control Panel to Classic mode
- Change the page file setting, so the server does not run out of virtual memory
- Support security certificate validation
- Partition disks appropriately for database, volumes, logs, cache, and ghost
- Add the appropriate roles

Details on these configurations are provided in the *IMPAX 6.5.1 AS300 Installation and Configuration Guide*.

3. Upgrading Windows Server 2008 to Windows Server 2008 SP2

(Topic number: 107471)

CAUTION!

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

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

To upgrade Windows Server 2008 to Windows Server 2008 SP2

1. Connect to the network or computer where you want to create the distribution folder.
2. In the shared folder, create a distribution folder for the service pack.
3. Copy Windows6.0-KB948465-*XXX*.exe into the distribution folder.

4. To install the service pack from a remote shared distribution folder, run **Windows6.0-KB948465-*XXX*.exe**.
5. Follow the instructions in the Setup Wizard.
6. When the installation process is complete, restart the computer.

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

4. Enabling Automatic Updates for Windows

(Topic number: 119644)

Automatic Updates allow Microsoft to automatically determine what critical system updates are needed for a system and to automatically download those updates. Only patches that Microsoft deems as critical system updates are downloaded. Critical updates are downloaded to C:\Program Files\WindowsUpdate\V4.When updates are downloaded, the Automatic Updates icon appears in the Windows taskbar.

If a critical update has a negative effect on the system, the critical update can be uninstalled using the Windows Add or Remove Programs dialog. Overall, Agfa believes that the risk to patient information is far greater if the system is not patched and does not have the prescribed critical system updates.

Enabling Automatic Updates for critical Windows XP or 2003 updates

(Topic number: 7701)

Note:

To provide a baseline to which the system can be restored in the event of a failure, before enabling Automatic Updates, we recommend that the system be “ghosted” using Symantec Ghost and that the database be backed up.

To enable Automatic Updates for critical Windows XP or 2003 updates

1. Open Control Panel.
2. Select **System**.
3. Switch to the **Automatic Updates** tab.
4. Select **Download updates for me, but let me choose when to install them**.
5. To apply the changes, click **OK**.
6. To verify that the Automatic Updates service is started, at a command prompt, type **net start**.
7. Verify that Automatic Updates is included in the list of services.

Tip:

Automatic Updates requires a direct Internet connection. If the system does not have a direct Internet connection, a local Software Update Server can be used instead. To set up a Software Update Server, contact your IT department.

Enabling Automatic Updates in Windows 2008

(Topic number: 107474)

Note:

To provide a baseline to which the system can be restored in the event of a failure, before enabling Automatic Updates, we recommend that the system be "ghosted" using Symantec Ghost and that the database be backed up.

To enable Automatic Updates in Windows 2008

1. Open Control Panel.
2. Select **Windows Update**.
3. Click **Change Settings**.
4. Select **Download updates, but let me choose whether to install them**.
5. To apply the changes, click **OK**.
6. If you see the message `To check for updates, you must first install an update for Windows Update`, click **Install now**.

   After the installation, you may have to restart the server.
7. To verify that the Automatic Updates service is started, at a command prompt, type **net start**.
8. Verify that Automatic Updates is included in the list of services.

Tip:

Automatic Updates requires a direct Internet connection. If the system does not have a direct Internet connection, a local Software Update Server can be used instead. To set up a Software Update Server, contact your IT department.

5. 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.

6. Enabling active content for the Knowledge Base

(Topic number: 7700)

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

Enabling remote access to Knowledge Bases

(Topic number: 10019)

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

To enable remote access to Knowledge Bases

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

   We recommend that https:// be used.
6. In the Add this website to the zone field, type or paste the name of the Application Server that the Knowledge Bases are installed on (**https://*server_name***).
7. Click **Add**.
8. Click **Close**.

9. Click **Custom Level**. In the Security Settings dialog, under Scripting, ensure that **Active scripting** is enabled. Click **OK**.
10. Click **OK**.

Enabling local access to Knowledge Bases

(Topic number: 10017)

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

To enable local access to Knowledge Bases

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

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

Upgrading an existing Database Server to IMPAX 6.5.1

4

If the existing Database Server has an adequate hardware profile, you can upgrade it to IMPAX 6.5.1, saving on the cost of new hardware.

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).

1. Upgrading SQL Server database software

(Topic number: 46572)

When upgrading to IMPAX 6.5.1, if you are currently on SQL Server 2000, and you want to continue using SQL Server, you **must** upgrade to SQL Server 2008 SP1. You cannot stay with SQL Server 2000. If you are already using SQL Server 2005, upgrading to SQL Server 2008 is optional.

Upgrading SQL Server 2000 to SQL Server 2008

(Topic number: 109391)

Before starting the upgrade from SQL Server 2000 to SQL Server 2008, ensure that you know the SQL Server 2000 sa database password, as you must enter it as part of the upgrade. Also ensure that you are logged into Windows as an administrator-level user.

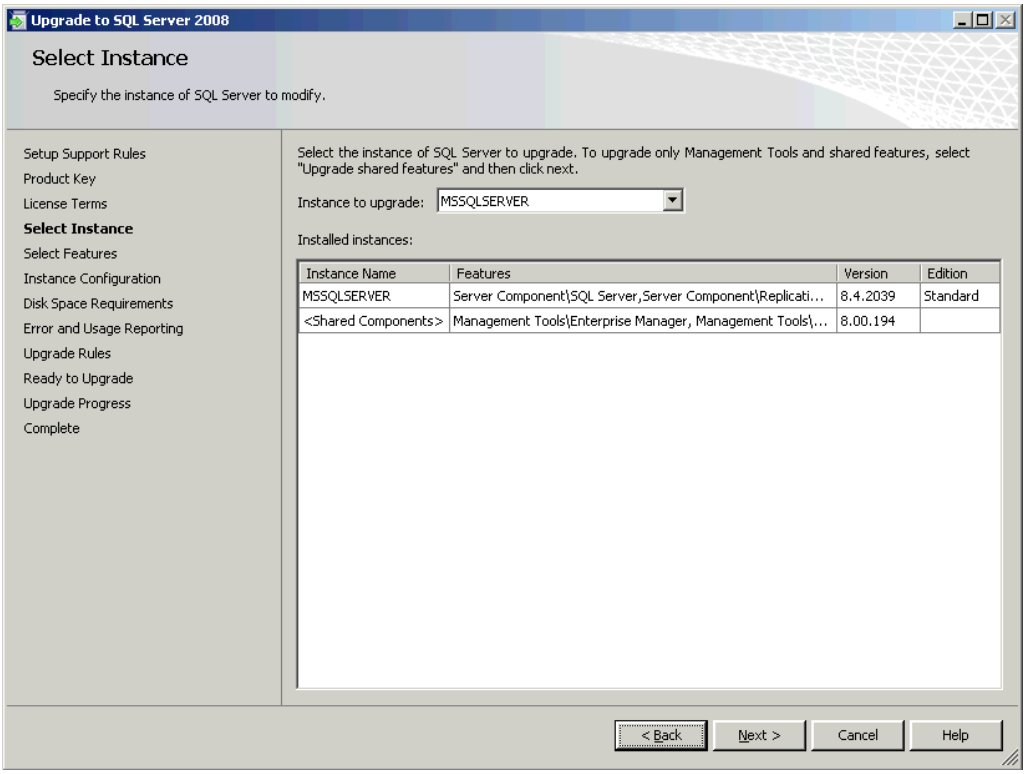
Upgrading to SQL Server 2008 requires running the same installer used for a new install of SQL Server 2008.

To upgrade SQL Server 2000 to SQL Server 2008

1. On the server you are upgrading, ensure that the Distributed Transaction Coordinator service is running:
   a. Open the Windows Administrative Tools and select **Services**.
   b. Select the **Distributed Transaction Coordination** service. If this service is not started, click **Start Service**.
2. Ensure that the SQLSERVERAGENT service is started.
3. To launch the installer, follow the instructions supplied with the SQL Server 2008 software.
4. When prompted, click **OK** and follow the on-screen instructions to install the Microsoft .NET Framework and updated Windows Installer. You might be asked to restart the server.
5. In the SQL Server Installation Center, select **Installation**, then select **Upgrade from SQL Server 2000 or SQL Server 2005**.

6. On the Setup Support Rules screen, ensure that all operations have completed successfully. Click **OK**.
7. On the next screen, enter the product key. Click **Next**.
8. When prompted, accept the Microsoft Software License Terms. Click **Next**.
9. On the Setup Support Files screen, click **Install**. After the support files are installed, click **Next**.
10. On the Setup Support Rules screen, ensure that all operations have completed successfully. Click **Next**.

11. In the Select Instance screen, check that **Instance to Upgrade** has been set to **MSSQLSERVER**. Click **Next**.



12. On the Select Features screen, click **Next**.
13. On the Instance Configuration screen, click **Next**.
14. Verify that the disk space requirements have been met. Click **Next**.
15. On the Server Configuration screen, click **Next**.
16. On the Full-text Upgrade screen, keep the default and click **Next**.
17. On the Error and Usage Reporting screen, click **Next**.
18. On the Upgrade Rules screen, check that no errors appear. Click **Next**.
19. On the Ready to Upgrade screen, click **Upgrade**.
20. Verify that the upgrade was successful, then click **Finish** and **Close**.
21. Restart the computer.

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

The next steps in the upgrade process are to stop the SQL Server services, then to install SQL Server 2008 SP1.

Stopping SQL Server 2008 services

(Topic number: 109422)

Before proceeding with the next task, stop the Windows SQL Server services, if they have been started.

To stop SQL Server 2008 services

1. Open the Windows Administrative Tools.
2. Select **Services**.
3. Select each of the following services in turn and click **Stop Service**, if needed:
    a. **SQL Server Full Text Search**
    b. **SQL Server Full Text Filter Daemon Launcher**
    c. **SQL Server Browser**
    d. **SQL Server Integration Services 10.0**
4. Close the Services window.

You can now install SQL Server 2008 SP1.

Upgrading SQL Server 2008 to SQL Server 2008 SP1

(Topic number: 107523)

The SQL Server 2008 SP1 executable file is **SQLServer2008SP1-KB968369-x86-ENU.exe** (32-bit). You must acquire this file from Microsoft; for example, you can download it from the Microsoft website at http://www.microsoft.com/downloads/en/details.aspx?FamilyID=66ab3dbb-bf3e-4f46-9559-ccc6a4f9dc19

Before running the installer, ensure that you know the sa (system administrator) database password, as you must enter it during the installation. Install the Service Pack after installing the software and stopping the SQL services.

To upgrade SQL Server 2008 to SQL Server 2008 SP1

1. Launch the SP1 installer.
2. If you see a security warning, click **Run**.
3. On the Welcome screen, click **Next**.
4. On the License Terms screen, select **I accept the agreement**. Click **Next**.
5. On the Feature Selection screen, accept the default selections. Click **Next**.
6. On the Check Files in Use screen, wait while the processes are identified. Then, click **Next**, even if some locked files are found.
7. On the Ready to Update screen, click **Update**.
8. On the Update Progress screen, wait until the components are upgraded or installed, then click **Next**.

9. If the Computer Reboot Required prompt appears, click **OK**.

   This will not automatically restart the computer.

10. On the Installation Complete screen, click **Close**.
11. Restart the computer.

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

CAUTION!

Do not attempt to start IMPAX at this point. If you start IMPAX now, the mvf user account will be locked and you will not be able to log into the MVF database. If the mvf user account becomes locked, see *Troubleshooting: Unlocking the mvf user account* (refer to page 131) for instructions on how to unlock the account.

2. Upgrading the IMPAX 5.2 or 5.3 database schema to IMPAX 6.5.1

(Topic number: 60244)

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 5.2 or 5.3 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 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

When upgrading the database, you will be prompted for the report source. When prompted, supply the value stored in the requesting_service field in the Connectivity Manager database. To prepare for the upgrade, identify this value in advance. See "Identifying the report source" (topic number 68030) in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

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.

Even if replacing the server with a new one, perform the upgrade on the existing server; you will later restore the upgraded database on the new server.

To upgrade the IMPAX database schema to IMPAX 6.5.1

1. On the Database Server, open a command prompt.

2. Change to the **C:\mvf-mig6\bin** directory.
3. If upgrading from IMPAX 5.2, type

   database-upgrade-script.bat -U sa -P *sapwd* -v 52

   If upgrading from IMPAX 5.3, type

   database-upgrade-script.bat -U sa -P *sapwd* -v 53

   where *sapwd* is the password for the 5.2 or 5.3 sa (system administrator) user. You must include the -v 52 or -v 53 parameter.

   If running this command on a server that will be replaced, and that does not have .NET installed, you will get a `block_named_pipes.exe: not finding the dynamic link library mscoree.dll` error. Ignore this error and continue with the upgrade, since the replacement server will be running Windows 2003 SP2, which installs .NET automatically.
4. At the prompt

   ```
   Ready to upgrade database to version 6.5.1. Do you want to proceed [y, n]?
   ```

   Type **y** to continue.
5. If prompted for the fully qualified host name of the login server, type the fully qualified host name of the Application Server.
6. When prompted for a report source, if the Connectivity Manager query you ran previously returned a single value, use that value as the report source. If the query returned multiple values for the requesting_service field, consult a Connectivity Manager integrator, as mappings may also need to be changed.

   If this Connectivity Manager receives data from multiple report sources, then a few requesting_service values may exist that match each report source.
7. Respond appropriately to other prompts that appear.

The database is upgraded.

In the IMPAX database, confirm that the values of the requesting_service field match those in the Connectivity Manager by typing

use mvf;

select distinct requesting_service from dosr_study;

3. Checking the status of SQL Server upgrades

(Topic number: 9914)

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 status of SQL Server upgrades

1. Open the log file C:\mvf-mig6\data\logs\migrate_database_to_IMPAX6.5.1.log
2. If the following warning appears in the log file, you can safely ignore it:

   ```
   Warning: The table 'CHANGE_CONTEXT_DETAIL' has been created but its maximum
   row size (8095) exceeds the maximum number of bytes per row (8060). INSERT
   or UPDATE of a row in this table will fail if the resulting row length exceeds
   8060 bytes.
   ```

3. Ensure that `Migration Complete Successful` appears at the end of the log file.

   If this message does not appear, review the rest of the log file to see where the upgrade failed. Solve the problem, then rerun the upgrade script.

4. Migrating data from the training server

(Topic number: 10237)

If you have configured worklists during the preparing to upgrade period, you can migrate these from the training server to the migrated database, instead of re-creating them. If you have migrated reports onto the training server, you can also migrate this data to the migrated database.

Taking the training server offline

(Topic number: 10239)

Before migrating data from the training server system, take the system offline.

To take the training server offline

1. On the training server system, launch the Administration Tools and log in as the **service** user.
2. On the Daily tab, select **Job Manager**. 
3. Select **All Queues**.
4. Click **Halt Queue**. 
5. Monitor each **Transmit** queue and wait for all outgoing jobs to finish.

   You cannot delete jobs in progress.
6. Select each Transmit queue and click **Halt Queue**.
7. To confirm that you want to halt the queue, click **Yes**.
8. To stop and disable all IMPAX services:
   a. Open a command prompt.
   b. Change to the **C:\mvf\bin** directory.
   c. Type **stopall.bat**.
   d. Type **removeall.bat**.

e. Exit the command prompt.

9. To prevent Client interaction, open the Windows Administrative Tools and select **Services**. Stop the **World Wide Web Publishing Service** (**IIS**).

Backing up the training server database

(Topic number: 10241)

CAUTION!

To mitigate the risk of selecting the wrong database when migrating worklist data and overwriting the training server database data, back up the training server database before migrating data from it.

To back up the training server database

1. Log into the training server as the **AgfaService** user.

   If you do not know the AgfaService password, you can run the passkey utility to find it: **passkey -M QUERY -u AgfaService**.

2. Stop the database by stopping the OracleServiceMVF Windows Service.
3. From the C:\oracle\product\10.2.0\db_1\database directory, copy the **PWDMVF.ora** and **spfileMVF.ora** to a different system.
4. Determine where the data files are located; for example, in E:\data\dbase.
5. Copy the entire **dbase** folder to a different system.

Migrating worklist and report data

(Topic number: 10243)

Before migrating data from the training server to the server where the database was upgraded, ensure that you have completed the following tasks:

- Installed the Migration Tools on the Application Server component of the training server cluster
- Created the pre-migration schema on the Database Server component of the training server cluster

These tasks are described in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

Note:

This topic assumes that the training server is running Oracle, while the production server is running SQL Server.

Also, if you are migrating worklist or report data from an Oracle database to a SQL Server database, first install Oracle 10.2.0.1 OLE drivers on the Application Server before migrating worklist or report migration. You can find instructions on how to install these drivers in the topic Installing 10.2.0.1 OLE drivers on the Application Server (refer to page 68).

You can now migrate worklist data, report data, or both from the training server to the server where the database was upgraded.

Note:

To ensure that failures do not occur, tools like SQLPlus, WinSQL, or Isql cannot be left connected to the MVF database (both the source and target MVF) when the MigrateTRServer tool is in use.

To migrate worklist and report data

1. On the Application Server, launch the Migrate training/traveling server data tool by running the **C:\mvf-mig6\MigrateTRServer\MigrateTRServer.exe** file.
2. If migrating worklist data, select the **Migrate Worklist Data** checkbox.
3. If migrating report data, select the **Migrate Report Data** checkbox.

   CAUTION!

   This utility overwrites reports on the destination server. Do not migrate report data from a training server unless all reports have been migrated to a training server that was receiving all patient, study and report updates, and was therefore acting as a production server for reports.

4. Under Source, supply the database information for the training server, as follows:
   a. Click **Modify**. 
   b. In the Data Link Properties dialog, select **Oracle Provider for OLE DB**. Click **Next**.
   c. In the Data Source field, type **mvf_ts.world** or the name of the tns entry in the tnsnames.ora file.
   d. Select **Use a specific name and password** and type the database user name—normally **dbadmin**.
   e. Click **OK**.
   f. In the Migrate training/traveling server data dialog, type the database password.
5. Under Destination, supply the database information for the production server (the upgraded IMPAX 6.5.1 server) as follows:
   a. Click **Modify**. 
   b. In the Data Link Properties dialog, select **Microsoft OLE DB Provider for SQL Server**. Click **Next**.
   c. In the Data Source field, type mvf_ts.world or the name of the tns entry that was created in tnsnames.ora.

d. Select **Use a specific name and password** and type the database user name—normally **sa**.

e. In the Select the database on the server field, type **mvf**.

f. Click **OK**.

g. In the Migrate training/traveling server data dialog, under Destination, type the database password.

6. If you have defined Source and Destination information for worklists and also need to migrate report data, under Reports, define the Source and Destination database information by following step 4 and step 5.

7. When all appropriate Source and Destination information is filled in, click **Migrate Data**.

   A DTSResults dialog opens showing the result of the data migration from the training to the production server. Scan it for any ERROR messages that you need to resolve.

8. When the migration is complete, close the DTSResults dialog.

   The Application Server caches the ref for the worklists. To update the refs from the migrated worklists, an IISRESET of the Application Server is needed; otherwise, when creating worklists, failures occur.

If you have migrated reports—not just worklists—you must next go to the Application Server, open the Business Services Configuration Tool, switch to the **Web Services** tab, and verify that the Report Info Sources settings are correct. For more information about these settings, refer to "Report source types: Reference" (topic number 11335) and "Modifying the settings of a report source" (topic number 11338) in the *IMPAX 6.5.1 Application Server Knowledge Base*.

Training server worklist or report data or both are now included in the production server database.

5. 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 5.2 *version*** or **Agfa IMPAX 5.3 *version***.
4. Click **Change/Remove**.
5. When prompted, type your name (minimum three characters). Click **Next**.
6. In the Confirmation dialog, click **OK**.
7. On the Maintenance Complete screen, click **Finish**.

8. Restart the server.

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

6. Determining a password for the AgfaService account

(Topic number: 7705)

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

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

7. 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.

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

AS300 installer log files

(Topic number: 6780)

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

8. Upgrading the IMPAX AS300 32-bit Database Server software

(Topic number: 6783)

Important!

This topic applies only when upgrading an existing Database Server.

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

Use the IMPAX installer to install the necessary packages on the system when upgrading an existing IMPAX server, including standalone and single-server stations. Descriptions of the packages are available in *32-bit AS300 installer packages reference* (refer to page 50).

Important!

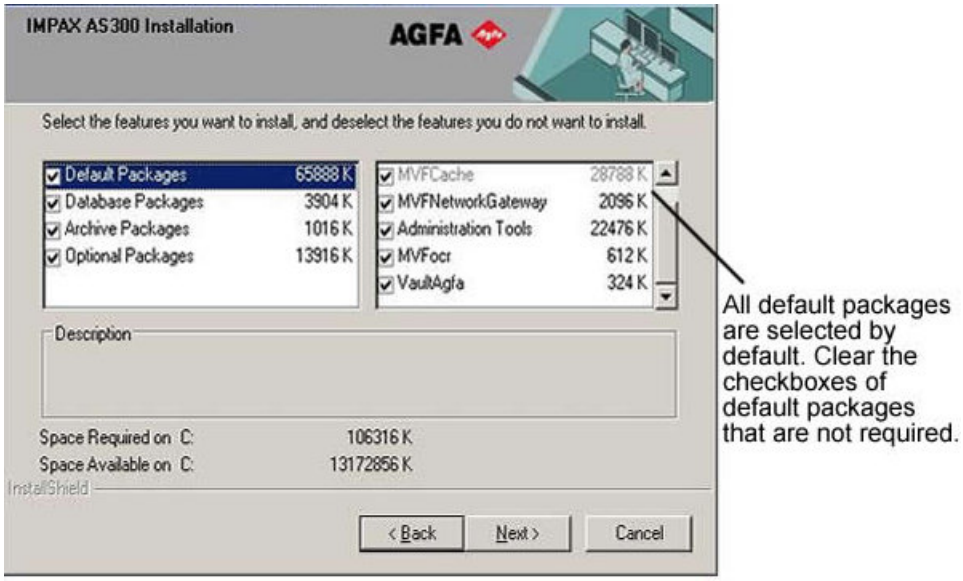
Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

To upgrade the IMPAX AS300 32-bit Database 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).

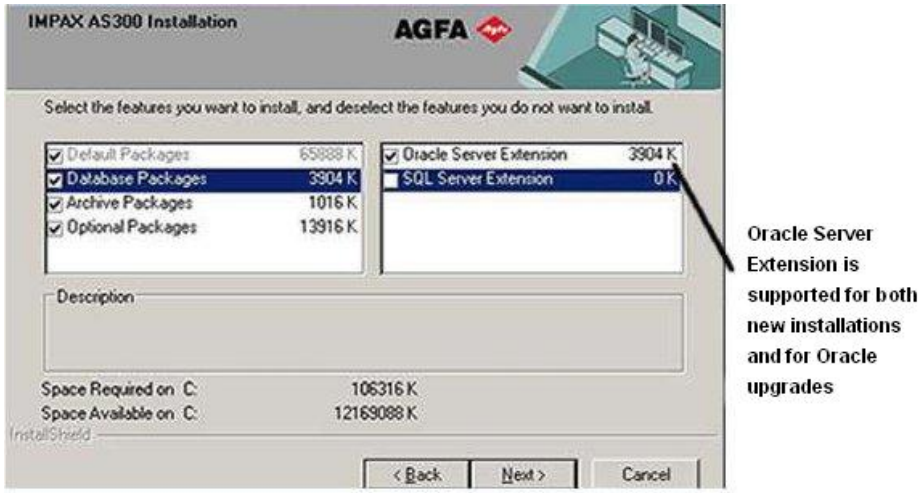
   This information is recorded in the installer log file.
4. On the Welcome screen, click **Next**.
5. On the Select features screen, all Default Packages are selected. Clear the checkboxes of any packages that should not be installed.

   For a single-host server, install all default packages except, potentially, the MVFocr package. For a dedicated Database Server, the MVFNetworkGateway package is not required, but can be installed.

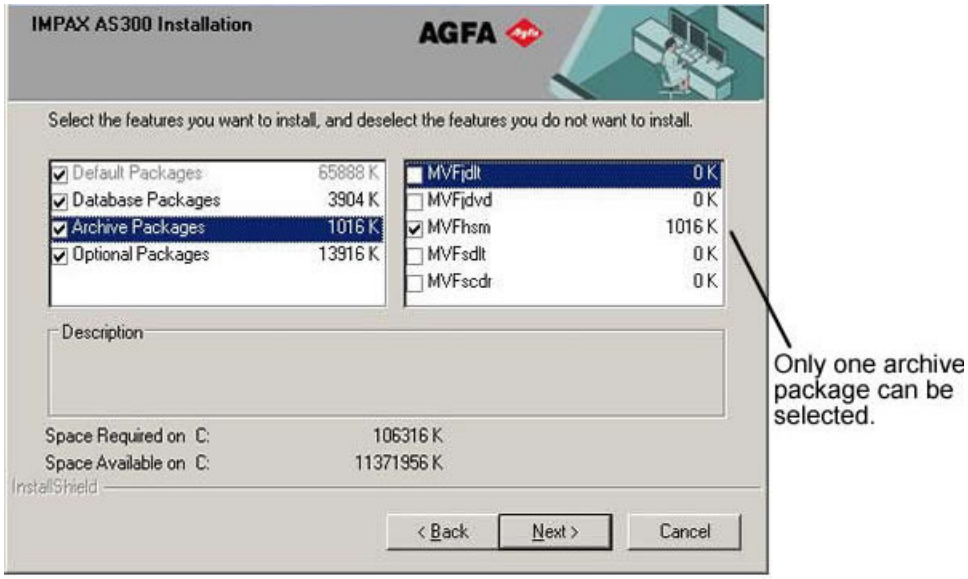


6. Select the **Database Packages** label.

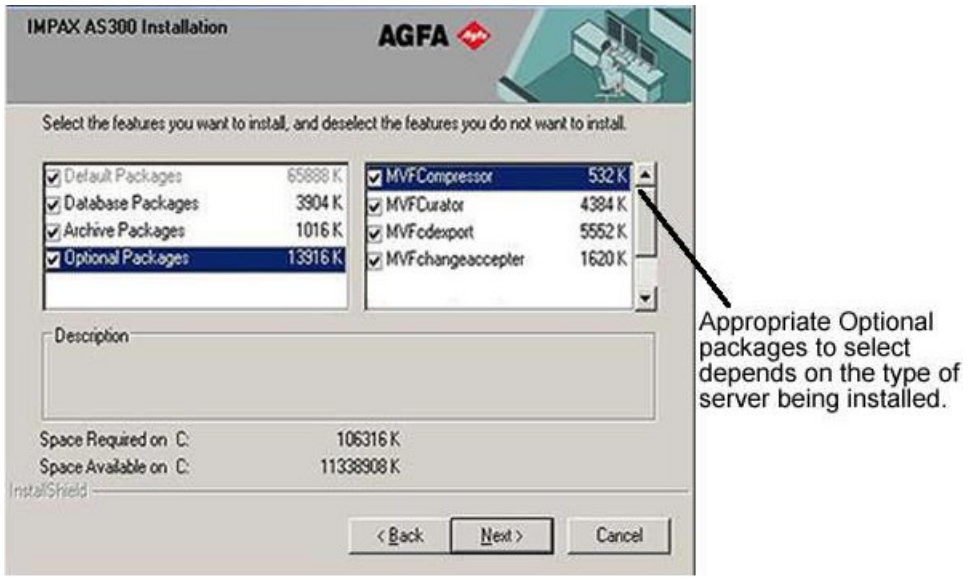
   Clear the **Oracle Server Extension** checkbox and select the **SQL Server Extension** checkbox.



7. For a dedicated Database Server (no archive), or if using PACS Store and Remember archiving only, clear the **Archive Packages** checkbox.



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



   - Select the **MVFCurator** and **MVFcdexport** checkboxes only if intending to install the Curator and CD Export server components on the Database Server rather than on a dedicated Curator server.
   - Select the **MVFpap** package only if the server is being used for archiving.
   - Clear the **MVFchangeaccepter** checkbox.
   - Do **not** select the MVForadg checkbox.

9. Click **Next**.

10. If a Network Gateway package was installed, browse to the location of the MVF license file and click **OK**.

    If the mvf.lic file is not located in C:\mvf, the file is copied to that location. A dialog informs you of the success of the copy task.

11. If an Archive package was installed, browse to the location of the 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.

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

    The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 50).

13. To confirm that the database is compatible, click **Yes**.
14. On the Ready to begin installation screen, click **Next**.

    The files are copied to the system.

15. To display the log file for the database scripts, when prompted, click **No**.
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.

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

9. Generating the AS300 portable password file

(Topic number: 7694)

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

To generate the AS300 portable password file

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

   passkey -M EXPORT -k *temporary_password*

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

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

CAUTION!

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

10. Updating the SQL Server registration

(Topic number: 7604)

To correctly register SQL Server with the Database Server software and set up permissions within SQL Server, update the SQL Server registration. To do so, you must be logged into Windows as an administrator-level user.

To update the SQL Server registration

1. Select **Start** > **All Programs** > **Microsoft SQL Server 2008**.
2. Right-click **SQL Server Management Studio** and select **Run as**.
3. In the Run as dialog, select **The following user**.
4. From the User name list, select **AgfaService**.
5. In the Password field, type the password for the AgfaService account and click **OK**.

11. Configuring Data Execution Prevention (DEP)

(Topic number: 7192)

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

Note:

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

To configure Data Execution Prevention (DEP)

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

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

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

Replacing an existing Database Server with a new station

5

When replacing the existing Database Server with a new one, you install all external and IMPAX 6.5.1 software in advance, during the preparing to upgrade period, saving you considerable time during the upgrade weekend.

For more details, refer to the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

1. Backing up the AS300 SQL 2000 database

(Topic number: 11497)

Back up the database so that you can restore it onto the new IMPAX 6.5.1 server.

Note:

Before backing up the database confirm that you have stopped the IMPAX services, emptied and halted all queues, and shut the database down. For more details, see the *Preparing to upgrade* (refer to page 22) tasks.

To back up the AS300 SQL 2000 database

1. On the server running the AS300 database, select **Start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**.
2. In the Explorer window of the Enterprise Manager, expand **Console Root** > **Microsoft SQL Servers** > **SQL Server Group** > ***server*** > **Databases** > **MVF**

   where *server* is the name of the SQL Server IMPAX is running under.
3. Select **Action** > **All Tasks** > **Backup database**.

4. In the SQL Server Backup screen, in the Backup section, select **Database–complete**.
5. Click **Add** and specify the directory to back up to.
6. To start the backup, click **OK**.
7. Exit the SQL Server Enterprise Manager.

2. Installing the 32-bit IMPAX 6.5.1 AS300 packages on a new Database Server

(Topic number: 125936)

Use the IMPAX installer to install the necessary AS300 packages on the system. These packages are described in *32-bit AS300 installer packages reference* (refer to page 50).

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

To install the 32-bit IMPAX 6.5.1 AS300 packages on a new Database Server

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

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

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

   For a single-host server, normally all Default Packages are required except, potentially, **MVFocr**.
6. Select the **Database Packages** label, then select the **SQL Server Extension** checkbox and clear the **Oracle Server Extension** checkbox.
7. Click **Next**.
8. When prompted, type the password for the AgfaService user.

   The password must follow the requirements outlined in *Determining a password for the AgfaService account* (refer to page 50).
9. On the Type of Install screen, select **Use existing database** and click **Next**.
10. On the Your existing database is compatible with this version screen, click **Yes**.

Note:

This is acceptable even though the mvf database has not yet been restored. The restore is done after the AS300 installation is completed.

11. On the Summary screen, to continue the installation, click **Next**.
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.

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

3. Restoring the upgraded database on a new Database Server

(Topic number: 7627)

CAUTION!

Perform this task only when replacing an existing server with a new server. Be very careful not to delete any live database files. Perform this procedure only on a new 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 replacing the existing server with a new server, you first install the IMPAX 6.5.1 server software on the new server. You then restore the backed-up database on the new server as described in this topic, before upgrading the schema.

Note:

Shut down all applications that usually connect to the SQL Server database. Under Services, stop the SQL Server agent. Also, shut down the SQL Server Query Analyzer when not using it as part of the restore process.

On the Application Server, open the Windows Administrative Tools and select **Services**. Right-click each of the following and select **Stop**: IMPAX App Server Data Manager, IMPAX Audit Event Log Manager, IMPAX Dicom Object Sender, IMPAX Distributed License Manager, IMPAX Messaging Service, and World Wide Web Publishing.

To restore the upgraded database on the new Database Server

1. Before starting the restore, confirm that the directory that will contain the mvf database files has the correct permission:
    a. In Windows Explorer, right-click the folder and select **Properties**.
    b. Switch to the **Security** tab.
    c. Click **Edit**.
    d. Click **Add**.
    e. Select **ImpaxSQLUser** and click **OK**.
    f. Grant **Full Control** to ImpaxSQLUser and click **OK**.

g. To close the Properties dialog, click **OK**.

2. If you are restoring from tape, insert the backup tape into the tape drive.
3. In the Explorer window of the SQL Server Management Studio, expand ***server*** > **Databases**.

   where *server* is the name of the SQL Server that IMPAX is running under.
4. Right-click **Database** and select **Restore Database**.
5. In the Destination for restore section, in the To database field, type **mvf**.
6. In the Source for restore section, select **From device** and specify the backup media and location.
7. Under Backup set to restore backup set, select the mvf database backup set.
8. Switch to the **Options** tab.
9. In the Restore the database files section, change the location of the data files as needed.
10. Select **Leave database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.** Click **OK**.

    The database is restored. After the restore is complete, a message confirms whether the restore was successful.
11. Create the mvf user login:
    a. Open SQL Server Management Studio.
    b. Select **Server** > **Security**.
    c. Right-click **Logins** and select **New login**.
    d. In the Login name field, type **mvf**.
    e. Select **SQL Server authentication** and in the Password field, type **mvf**.
    f. Clear the **Enforce password policy** checkbox and click **OK**.
12. Restore the mvf user permissions:
    a. Open SQL Server Management Studio.
    b. Open a new query window.
    c. Select **File** > **Open** and browse to C:\mvf\etc.
    d. Select **recreate_user_mvf.sql** and click **Open**.
    e. To execute the script, press **F5** or click **Execute**.

4. Upgrading the IMPAX 5.2 or 5.3 database schema to IMPAX 6.5.1

(Topic number: 60244)

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 5.2 or 5.3 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 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

When upgrading the database, you will be prompted for the report source. When prompted, supply the value stored in the requesting_service field in the Connectivity Manager database. To prepare for the upgrade, identify this value in advance. See "Identifying the report source" (topic number 68030) in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

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.

Even if replacing the server with a new one, perform the upgrade on the existing server; you will later restore the upgraded database on the new server.

To upgrade the IMPAX database schema to IMPAX 6.5.1

1. On the Database Server, open a command prompt.
2. Change to the **C:\mvf-mig6\bin** directory.
3. If upgrading from IMPAX 5.2, type

   database-upgrade-script.bat -U sa -P *sapwd* -v 52

   If upgrading from IMPAX 5.3, type

   database-upgrade-script.bat -U sa -P *sapwd* -v 53

   where *sapwd* is the password for the 5.2 or 5.3 sa (system administrator) user. You must include the -v 52 or -v 53 parameter.

   If running this command on a server that will be replaced, and that does not have .NET installed, you will get a `block_named_pipes.exe: not finding the dynamic link library mscoree.dll` error. Ignore this error and continue with the upgrade, since the replacement server will be running Windows 2003 SP2, which installs .NET automatically.

4. At the prompt

   ```
   Ready to upgrade database to version 6.5.1. Do you want to proceed [y, n]?
   ```

   Type **y** to continue.

5. If prompted for the fully qualified host name of the login server, type the fully qualified host name of the Application Server.
6. When prompted for a report source, if the Connectivity Manager query you ran previously returned a single value, use that value as the report source. If the query returned multiple values for the requesting_service field, consult a Connectivity Manager integrator, as mappings may also need to be changed.

   If this Connectivity Manager receives data from multiple report sources, then a few requesting_service values may exist that match each report source.
7. Respond appropriately to other prompts that appear.

The database is upgraded.

In the IMPAX database, confirm that the values of the requesting_service field match those in the Connectivity Manager by typing

use mvf;

select distinct requesting_service from dosr_study;

5. Checking the status of SQL Server upgrades

(Topic number: 9914)

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 status of SQL Server upgrades

1. Open the log file C:\mvf-mig6\data\logs\migrate_database_to_IMPAX6.5.1.log
2. If the following warning appears in the log file, you can safely ignore it:

   ```
   Warning: The table 'CHANGE_CONTEXT_DETAIL' has been created but its maximum
   row size (8095) exceeds the maximum number of bytes per row (8060). INSERT
   or UPDATE of a row in this table will fail if the resulting row length exceeds
   8060 bytes.
   ```

3. Ensure that `Migration Complete Successful` appears at the end of the log file.

   If this message does not appear, review the rest of the log file to see where the upgrade failed. Solve the problem, then rerun the upgrade script.

6. Migrating data from the training server

(Topic number: 10237)

If you have configured worklists during the preparing to upgrade period, you can migrate these from the training server to the migrated database, instead of re-creating them. If you have migrated reports onto the training server, you can also migrate this data to the migrated database.

Taking the training server offline

(Topic number: 10239)

Before migrating data from the training server system, take the system offline.

To take the training server offline

1. On the training server system, launch the Administration Tools and log in as the **service** user.
2. On the Daily tab, select **Job Manager**. 
3. Select **All Queues**.
4. Click **Halt Queue**. 
5. Monitor each **Transmit** queue and wait for all outgoing jobs to finish.

   You cannot delete jobs in progress.
6. Select each Transmit queue and click **Halt Queue**.
7. To confirm that you want to halt the queue, click **Yes**.
8. To stop and disable all IMPAX services:
   a. Open a command prompt.
   b. Change to the **C:\mvf\bin** directory.
   c. Type **stopall.bat**.
   d. Type **removeall.bat**.
   e. Exit the command prompt.
9. To prevent Client interaction, open the Windows Administrative Tools and select **Services**. Stop the **World Wide Web Publishing Service** (**IIS**).

Backing up the training server database

(Topic number: 10241)

CAUTION!

To mitigate the risk of selecting the wrong database when migrating worklist data and overwriting the training server database data, back up the training server database before migrating data from it.

To back up the training server database

1. Log into the training server as the **AgfaService** user.

   If you do not know the AgfaService password, you can run the passkey utility to find it: **passkey -M QUERY -u AgfaService**.

2. Stop the database by stopping the OracleServiceMVF Windows Service.
3. From the C:\oracle\product\10.2.0\db_1\database directory, copy the **PWDMVF.ora** and **spfileMVF.ora** to a different system.
4. Determine where the data files are located; for example, in E:\data\dbase.
5. Copy the entire **dbase** folder to a different system.

Migrating worklist and report data

(Topic number: 10243)

Before migrating data from the training server to the server where the database was upgraded, ensure that you have completed the following tasks:

- Installed the Migration Tools on the Application Server component of the training server cluster
- Created the pre-migration schema on the Database Server component of the training server cluster

These tasks are described in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

Note:

This topic assumes that the training server is running Oracle, while the production server is running SQL Server.

Also, if you are migrating worklist or report data from an Oracle database to a SQL Server database, first install Oracle 10.2.0.1 OLE drivers on the Application Server before migrating worklist or report migration. You can find instructions on how to install these drivers in the topic Installing 10.2.0.1 OLE drivers on the Application Server (refer to page 68).

You can now migrate worklist data, report data, or both from the training server to the server where the database was upgraded.

Note:

To ensure that failures do not occur, tools like SQLPlus, WinSQL, or Isql cannot be left connected to the MVF database (both the source and target MVF) when the MigrateTRServer tool is in use.

To migrate worklist and report data

1. On the Application Server, launch the Migrate training/traveling server data tool by running the **C:\mvf-mig6\MigrateTRServer\MigrateTRServer.exe** file.
2. If migrating worklist data, select the **Migrate Worklist Data** checkbox.
3. If migrating report data, select the **Migrate Report Data** checkbox.

   CAUTION!

   This utility overwrites reports on the destination server. Do not migrate report data from a training server unless all reports have been migrated to a training server that was receiving all patient, study and report updates, and was therefore acting as a production server for reports.

4. Under Source, supply the database information for the training server, as follows:
   a. Click **Modify**. 
   b. In the Data Link Properties dialog, select **Oracle Provider for OLE DB**. Click **Next**.
   c. In the Data Source field, type **mvf_ts.world** or the name of the tns entry in the tnsnames.ora file.
   d. Select **Use a specific name and password** and type the database user name—normally **dbadmin**.
   e. Click **OK**.
   f. In the Migrate training/traveling server data dialog, type the database password.
5. Under Destination, supply the database information for the production server (the upgraded IMPAX 6.5.1 server) as follows:
   a. Click **Modify**. 
   b. In the Data Link Properties dialog, select **Microsoft OLE DB Provider for SQL Server**. Click **Next**.
   c. In the Data Source field, type mvf_ts.world or the name of the tns entry that was created in tnsnames.ora.
   d. Select **Use a specific name and password** and type the database user name—normally **sa**.
   e. In the Select the database on the server field, type **mvf**.

f. Click **OK**.

g. In the Migrate training/traveling server data dialog, under Destination, type the database password.

6. If you have defined Source and Destination information for worklists and also need to migrate report data, under Reports, define the Source and Destination database information by following step 4 and step 5.
7. When all appropriate Source and Destination information is filled in, click **Migrate Data**.

   A DTSResults dialog opens showing the result of the data migration from the training to the production server. Scan it for any ERROR messages that you need to resolve.
8. When the migration is complete, close the DTSResults dialog.

   The Application Server caches the ref for the worklists. To update the refs from the migrated worklists, an IISRESET of the Application Server is needed; otherwise, when creating worklists, failures occur.

If you have migrated reports—not just worklists—you must next go to the Application Server, open the Business Services Configuration Tool, switch to the **Web Services** tab, and verify that the Report Info Sources settings are correct. For more information about these settings, refer to "Report source types: Reference" (topic number 11335) and "Modifying the settings of a report source" (topic number 11338) in the *IMPAX 6.5.1 Application Server Knowledge Base*.

Training server worklist or report data or both are now included in the production server database.

Installing Oracle 10.2.0.1 OLE drivers on the Application Server

(Topic number: 114114)

If you are migrating worklist or report data from an Oracle database to a SQL Server database, you must install Oracle 10.2.0.1 OLE Drivers on the Application Server before starting the worklist or report migration.

Note:

Perform this task on an Application Server that does not already have an Oracle client installed. If an Oracle Client is already installed on the Application Server, use the training/travelling server data tool on a machine that does not have the Oracle client installed.

To install Oracle 10.2.0.1 OLE drivers on the Application Server

1. Unzip the 10201_client_win32.zip file.
2. Run the unzipped Oracle 10g Client installer.
3. Click **Install** to open the Universal Installer.
4. In the Welcome dialog, click **Next**.
5. In the Select Installation Type dialog, select **Custom**, then click **Next**.
6. In the Specify Home Details dialog, change the path as needed and click **Next**.

7. In the Available Product Components dialog, select **Oracle Objects for OLE 10.2.0.1.0**, **Oracle ODBC Driver 10.2.0.1.0**, and **Oracle Provider for OLE DB 10.2.0.1.0** only.
8. Click **Next**.
9. Click **Next** again, then click **Install**.

After installation, create a tnsnames.ora file in the C:\oracle\product\10.2.0\client_1\NETWORK\ADMIN directory and add the following code to the file:

```
mvf_ts.world =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (COMMUNITY = impax.world)(PROTOCOL = TCP)(HOST =
name_of_training_server)(PORT = 1521)))
(CONNECT_DATA =
(SID=MVF)
))
```

7. Generating the AS300 portable password file

(Topic number: 7694)

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

To generate the AS300 portable password file

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

   passkey -M EXPORT -k *temporary_password*

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

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

CAUTION!

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

Upgrading other AS300 servers to IMPAX 6.5.1

6

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).

These procedures are relevant when:

- Upgrading the site in a multi-host or mixed-configuration.

  and

- Upgrading existing AS300 Archive Server and Network Gateway stations to IMPAX 6.5.1, rather than replacing them with new stations.

Note:

If upgrading the site in a single-host configuration or replacing existing stations with new ones (on which IMPAX 6.5.1 software can be installed in advance), Network Gateway, and Archive Server upgrades are not required.

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 5.2 *version*** or **Agfa IMPAX 5.3 *version***.
4. Click **Change/Remove**.
5. When prompted, type your name (minimum three characters). Click **Next**.
6. In the Confirmation dialog, click **OK**.
7. On the Maintenance Complete screen, click **Finish**.
8. Restart the server.

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

2. Configuring the ODBC connection to the SQL Database Server

(Topic number: 6813)

Configure the ODBC connection to the SQL Database Server for Windows. This connection is required for the Archive Server, Network Gateway, and Curator to communicate with an AS300 Database Server running under SQL Server (and therefore does not apply if using an AS300 Oracle for Windows database or if connecting to an AS3000 Database Server).

To configure the ODBC connection to the SQL Database Server

1. On the server to connect, open the Windows Administrative Tool and select **Data Sources (ODBC)**.
2. Switch to the **System DSN** tab.
3. Click **Add**.
4. In the Create New Data Source dialog, select **SQL Server**.
5. Click **Finish**.
6. In the Name field, type **mvf**.
7. In the Description field, type **mvf**.
8. In the Server list, type or select the Database Server name. Click **Next**.
9. If asked whether to overwrite the existing MVF_SQL, click **Yes**.
10. Select the **SQL Server Authentication** option.
11. In the Login ID and Password fields, type the username and password for the mvf user.

    Ensure that all systems have the same username and password for the Database Server.
12. Click **Client Configuration**.
13. In the Add Network Library Configuration dialog, select **TCP/IP**. Click **OK**.

14. Click **Next**.
15. Select the **Change the default database to** checkbox.
16. From the list, select **mvf**. Click **Next**.
17. Clear the **Perform translation for character data** checkbox.
18. Click **Finish**.
19. To test the connection, click **Test Connection**.
20. In the ODBC Driver Connect dialog, type the password for the mvf user and click **OK**.
21. When prompted that the connection was successful, click **OK**.
22. To close the Oracle ODBC Driver Configuration dialog, click **OK**.
23. To close the ODBC Data Source Administrator window, click **OK**.

3. 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 50).

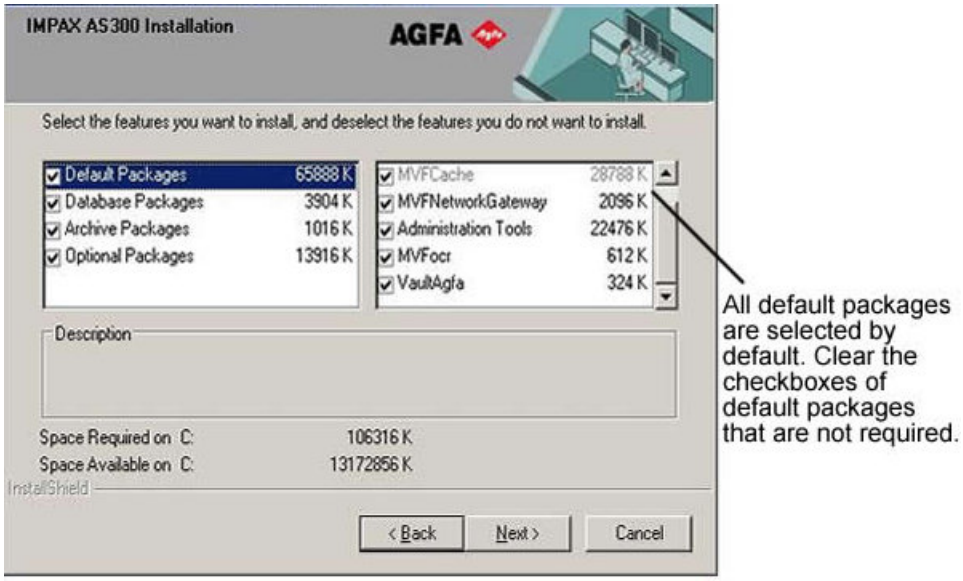
To install the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages

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.

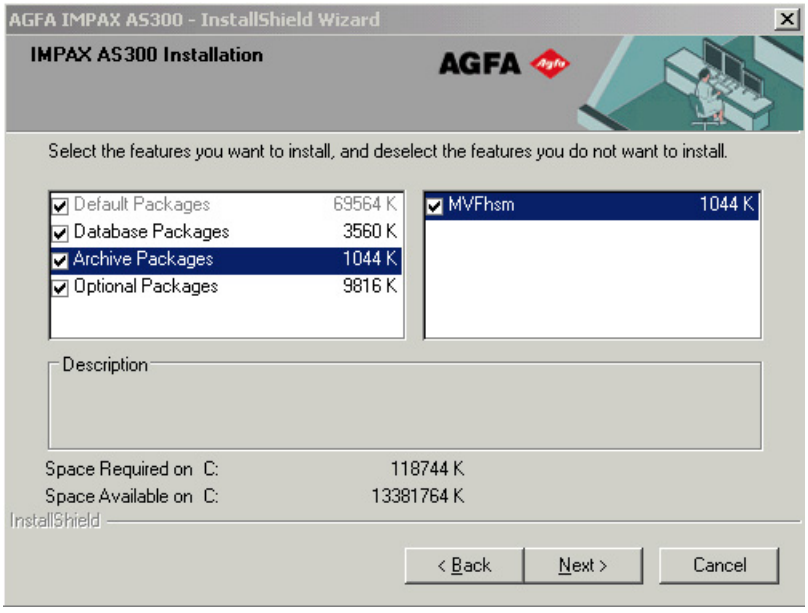
   If installing a Network Gateway or an Archive Server/Network Gateway combination, you can normally leave all the default packages selected.

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

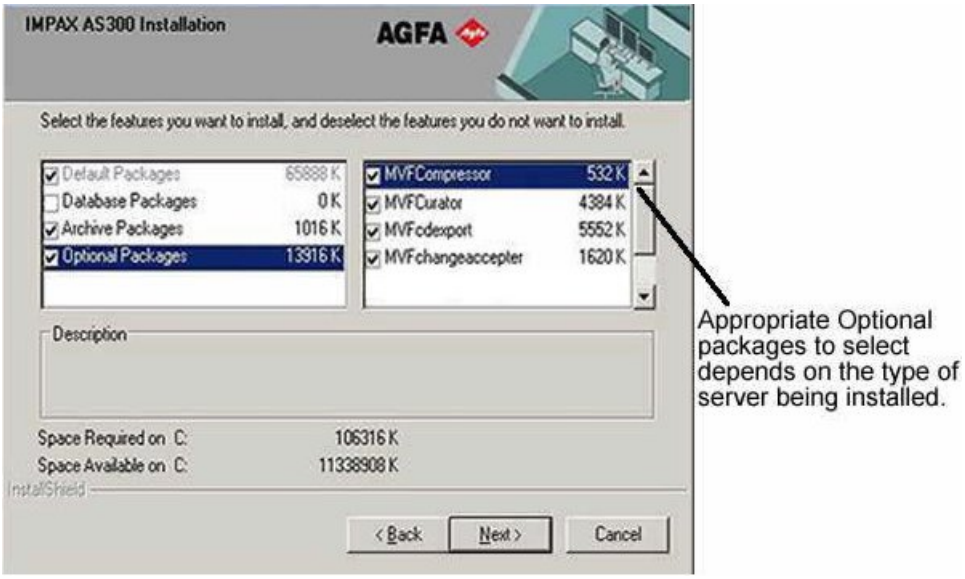


6. Clear the **Database Packages** checkbox.
7. For Archive Servers, select the **Archive Package** label. The MVFhsm is the only archive package listed and is selected by default. If not using an HSM archive, clear the **MVFhsm** checkbox; otherwise, keep it selected.

   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.

4. 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*.

5. Configuring Data Execution Prevention (DEP)

(Topic number: 7192)

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

Note:

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

To configure Data Execution Prevention (DEP)

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

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

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

Reconfiguring the Application Server and Curator

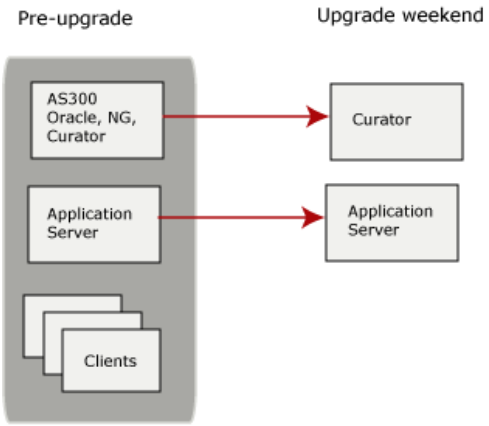
7

After the Server components are upgraded, you must configure the Application Server to work with the production server instead of the training server and possibly convert the training server into a Curator.

1. Reconfiguring the Application Server

(Topic number: 6809)

During the preparing to upgrade period, the station intended to serve as the new Application Server for the site is connected to a temporary AS300 single-host station. (This configuration option is described in the "Installing a training server cluster" section of the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*; also see the Training server configurations diagram.)



User migrations and configurations are performed on the Application Server (as described in the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*) and worklist and report data can be migrated from the training server (described in *Migrating data from the training server* (refer to page 65)).

After all these migrations are complete, reconfigure the Application Server to connect to the production database instead of the training server. Several steps are required:

1. Disable the connection to the temporary IMPAX 6.5.1 database, to the IMPAX 5.2 or 5.3 database and, if applicable, to the WEB1000 Server.
2. Connect to the production IMPAX 6.5.1 database.
3. Import the portable password file generated from the production 6.5.1 Database Server.
4. Set the password and account lockout policies.
5. Connect to a non-queryable RIS and remove an IP address from the IP filtering list.

   To connect to another type of RIS (local or remote Agfa RIS or a queryable RIS), refer to instructions in the *IMPAX 6.5.1 Application Server Knowledge Base*.
6. Perform other Application Server configurations that could not be completed during the preparing to upgrade period, such as managing web services, setting up Healthcheck, and managing SSL certificates.

Details on each of these steps follow.

Disabling SQL connections

(Topic number: 6802)

The Application Server is currently configured to communicate with the IMPAX 5.2 or 5.3 SQL Server database. Disable the connections to those servers, and to the WEB1000 Server station, if you have set that up.

To disable SQL connections

1. On the Application Server, open the Windows Administrative Tools and select **Data Sources (ODBC)**.
2. Switch to the **System DSN** tab.
3. Select the name of the IMPAX 5.2 or 5.3 database.
4. Click **Remove**. Confirm the removal.
5. If a connection to the WEB1000 Server was set up, select the name of that database and click **Remove**. Confirm the removal.
6. Click **OK**.

Connecting to the IMPAX 6.5.1 SQL Server database

(Topic number: 6811)

You must now configure the Application Server for the migrated IMPAX 6.5.1 database.

To connect to the IMPAX 6.5.1 SQL Server database

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

    If the test fails, verify that the SQL Server Name is correct and test the connection again.
28. Click **Apply**.

Importing the portable password file to the Application Server

(Topic number: 6877)

You must now import the portable password file generated from the migrated IMPAX 6.5.1 Database Server to the Application Server.

To import the portable password file to the Application Server

1. Select **Start** > **All Programs** > **Agfa Healthcare** > **Business Services** > **Configuration Tool**.
2. In the IMPAX Business Services Configuration tool, switch to the **Security** tab.
3. Click **Import Password**.
4. Navigate to the mvf.portable.psd file and click **Open**.
5. At the prompt, enter the temporary password identified when creating the portable password. Click **OK**.
6. At the confirmation message, click **OK**.
7. Click **Apply**.

CAUTION!

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

Setting the password and account lockout policies

(Topic number: 6853)

To perform the user migrations, the password and account lockout policies were disabled. You can now reset these according to the site's IT department policies.

For information on what these policies are and how to reset them, refer to "Setting the password and account lockout policies" (topic number 11372) and "Password and account lockout policies: Reference" (topic number 11366) in the *IMPAX 6.5.1 Application Server Knowledge Base*.

Connecting the Application Server to a non-queryable non-IMPAX RIS

(Topic number: 11343)

A non-queryable RIS supports only one-way communication between the RIS and IMPAX. A non-queryable RIS sends unsolicited HL7 messages for orders and reports to the Connectivity Manager, and the Connectivity Manager parses the HL7 messages and sends them to the IMPAX database for storage. To display the information available from a non-queryable RIS in the IMPAX Client Text area, connect to a non-queryable RIS through the Connectivity Manager.

Note:

To connect to another type of RIS (local or remote IMPAX RIS or a queryable RIS), refer to instructions in the *IMPAX 6.5.1 Application Server Knowledge Base*.

To connect the Application Server to a non-queryable non-IMPAX RIS

1. Configure the custom RIS mappings in Connectivity Manager.
2. Open the Business Services Configuration Tool.
3. Switch to the **Web Services** tab.
4. In the Report Info Sources area, click **Add**.
5. To check the value of the requesting_service field in the Connectivity Manager database, type

   use mcf;

   select distinct requesting_service from mcf_service_request;

   Note:

   If this query returns a single value, make note of it. If this query returns multiple values for the requesting_service field, consult a Connectivity Manager integrator, as mappings may also have to be changed. If this Connectivity Manager receives data from multiple report sources, there may be several requesting_service values that match each report source.

6. In the Edit Report Source dialog, type the requesting_service value returned in the previous step into the Report Source Provider field.

   Note:

   This field is case-sensitive. A maximum of 64 characters can be entered in this field.

7. From the RIS Type list, select **Connectivity Manager Non-Queryable RIS**. Click **OK**.
8. Under Connectivity Manager IP Filtering, in the Grant Access to IP field, type the IP address of the Connectivity Manager and click **Add**.

   If the Connectivity Manager uses a proxy server, type the IP address of the proxy server. To specify multiple IP addresses, separate each with a comma.
9. To close the Business Services Configuration Tool, click **OK**.

Performing other Application Server configurations

(Topic number: 6858)

At this point, you can complete any other Business Service configurations you could not complete during the preparing to upgrade period, such as managing web services, setting up Healthcheck, and configuring the image upload server. For details on these configurations, refer to the *IMPAX 6.5.1 Application Server Knowledge Base*.

2. Reconfiguring the Curator

(Topic number: 10172)

For IMPAX 5.2 or 5.3 upgrades, the Curator station has likely been set up as a single-host station, for use as part of the training server cluster during the preparing to upgrade period. In this case, you must uninstall the AS300 software from it, then reinstall the AS300 software with only the Curator packages selected.

If the Curator was not initially set up as a single-host station, you can install Curator now by following the procedures in the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide*.

Uninstalling IMPAX 6.5.1 Server

(Topic number: 7605)

If the Curator station was initially staged as an IMPAX 6.5.1 AS300 single-host station during the pre-upgrade period, change the AS300 software installation to remove the database packages and add the Curator packages.

To uninstall IMPAX 6.5.1 Server

1. Ensure that the training server (the future Curator station) is offline (refer to page 65).
2. Open Control Panel.
3. Depending on the version of Windows, select **Add or Remove Programs** or **Programs and Features**.
4. Under Currently installed programs, select **AGFA IMPAX AS300**.
5. Click **Change**.
6. At the prompt, type your name and click **Next**.
7. At the Welcome dialog, select **Modify**. Click **Next**.
8. Clear the checkboxes of all AS300 packages other than **MVFCore**, **MVFCurator**, and **MVFcdexport**.

   Where a single-host Database Server has almost all available AS300 packages installed, a Curator server requires only these three packages.
9. Click **Next**.
10. In the Maintenance Complete dialog, select **Yes, I want to restart my computer now** and click **Finish**.
11. If no longer required on this server, you can also delete any Server license files stored in the C:\mvf directory.

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

Uninstalling Oracle on Windows

(Topic number: 65064)

Oracle Server is no longer required on the Curator server (though Oracle Client is, if using an Oracle database). Remove the Oracle Server software.

CAUTION!

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

To uninstall Oracle on Windows

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

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

   C:\oracle

   C:\Program Files\Oracle

   C:\OracleDatabase (keep only if reinstalling the same version of oracle)
10. Run regedit and delete the **HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE** key.
11. Delete all files in the C:\cygwin\tmp directory.
12. Delete all files in C:\cygwin\var\tmp directory.
13. Delete the **C:\installOracleInfo** file.
14. Restart the server.

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

You can now install Oracle Client for Windows (refer to page 84) on this server.

Installing and configuring the Oracle 10g Client for Windows

(Topic number: 6790)

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

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

Important!

Before installing the Oracle Client, disable virus protection software.

To install and configure the Oracle 10g Client for Windows

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

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

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

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

Note:

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

Configuring the ODBC connection to the SQL Database Server

(Topic number: 6813)

Configure the ODBC connection to the SQL Database Server for Windows. This connection is required for the Archive Server, Network Gateway, and Curator to communicate with an AS300 Database Server running under SQL Server (and therefore does not apply if using an AS300 Oracle for Windows database or if connecting to an AS3000 Database Server).

To configure the ODBC connection to the SQL Database Server

1. On the server to connect, open the Windows Administrative Tool and select **Data Sources (ODBC)**.
2. Switch to the **System DSN** tab.
3. Click **Add**.
4. In the Create New Data Source dialog, select **SQL Server**.
5. Click **Finish**.
6. In the Name field, type **mvf**.
7. In the Description field, type **mvf**.
8. In the Server list, type or select the Database Server name. Click **Next**.
9. If asked whether to overwrite the existing MVF_SQL, click **Yes**.
10. Select the **SQL Server Authentication** option.
11. In the Login ID and Password fields, type the username and password for the mvf user.

    Ensure that all systems have the same username and password for the Database Server.
12. Click **Client Configuration**.
13. In the Add Network Library Configuration dialog, select **TCP/IP**. Click **OK**.
14. Click **Next**.
15. Select the **Change the default database to** checkbox.
16. From the list, select **mvf**. Click **Next**.
17. Clear the **Perform translation for character data** checkbox.
18. Click **Finish**.
19. To test the connection, click **Test Connection**.
20. In the ODBC Driver Connect dialog, type the password for the mvf user and click **OK**.
21. When prompted that the connection was successful, click **OK**.
22. To close the Oracle ODBC Driver Configuration dialog, click **OK**.
23. To close the ODBC Data Source Administrator window, click **OK**.

Setting up the Curator web cache

(Topic number: 7029)

If you did not create a web cache for Curator when you configured the Database Server, create the web cache now. The cache must be created from the Database Server.

Note:

For Autopilot to correctly monitor cache space, each cache must be on its own partition.

Although multiple Curators may be installed, each Curator places web representations of objects into the same web cache. This web cache is owned by the master Curator and is managed by the Autopilot running on the master Curator.

Creating a web cache volume

(Topic number: 7069)

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

To create a web cache volume

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

Configuring cache folder permissions for remote caches and NAS

(Topic number: 7068)

If the cache is hosted remotely or if you are setting up network area storage (NAS), after the cache is created, create a user account for the ImpaxServerUser on the system hosting the cache.

To configure cache folder permissions for remote caches and NAS

1. On the 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 root user) directory.
3. To obtain the password for the ImpaxServerUser, type

   passkey -M QUERY -u ImpaxServerUser (AS300) or **./passkey -M QUERY -u ImpaxServerUser**(AS3000)

   This password is used for the ImpaxServerUser account on the remote machine.
4. If the remote web cache is hosted on a Windows-based system, log into the machine as an administrator-level user. Using the built-in Windows 2003 Server security configuration, create an account for the ImpaxServerUser that uses the same password as the account on the Database Server.

   If the web cache is hosted on a Solaris-based system, install and configure a subprocess such as NFS or SAMBA.
5. If an ImpaxServerUser account cannot be used on the remote cache but rather a domain user needs to be used, create the domain user and add this user to the ImpaxServerGroup on the IMPAX machines requiring access (for example, the Curator). Update the IMPAX services to log in as this new domain user.

Configuring web cache folder permissions

(Topic number: 7077)

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

To configure web cache folder permissions on Windows Server 2003

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

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

To configure web cache folder permissions on Windows Server 2008

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

Preparing the web cache

(Topic number: 10178)

Using CLUI, you can prepare the last few weeks of studies, so that recent wavelets are readily available in the Curator web cache. You can do this by date range or based on a list of study references.

Preparing studies within a date range

(Topic number: 58333)

One way to prepare studies in the web cache is to specify them by date range.

To prepare studies within a date range

1. To store all study_refs into variable *a*, in CLUI, type

   save_refs a select study_ref from dosr_study where study_date >= '*start_date*' and study_date <= '*end_date*'

   where the date format to use is *yyyymmdd*; for example, **20080928** for 28 September 2008.
2. To enter menu mode, type **Go menu**.
3. Select **1** for Study Manager.
4. Select **5** for Prepare Study.
5. At the prompt for the list of studies to process, enter **a** to reference the save_refs list of studies.

Preparing studies based on a list of study references

(Topic number: 58336)

Another way to prepare studies for the Curator web cache is to specify them based on study reference.

To prepare studies based on a list of study references

1. In CLUI, specify the files to prepare with this command:

   study prepare *study_ref_1 study_ref_2... study_ref_n*

In both cases, a set of PREPARE jobs is created to be processed over time.

Performing other Curator configurations

(Topic number: 60423)

Depending on site requirements, other Curator configurations may be required, or slave Curators may need to be installed. For details on these, refer to the *IMPAX 6.5.1 Curator and CD Export Server Installation Guide* and the Curator component of the *IMPAX 6.5.1 Server Knowledge Base*.

Completing the upgrade and migration

8

To complete the migration, Clients need upgrading, and various other configurations and upgrades must be performed.

1. 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*.

2. 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*.

3. Changing the SQL Server administrator (sa) password

(Topic number: 7738)

Important!

This topic applies only to Database Servers (including single-host, standalone, and single-server configurations).

The IMPAX installation changes the default sa password to a randomly generated string of characters. This greatly increases the security of the system; however, the password can still be obtained through other methods.

To ensure that your system is as secure as possible, we recommend updating the sa password to a strong password that is known only by the site administrator.

Note:

Do this only after the Application Server software has been installed and configured.

To change the SQL Server administrator password

1. On an IMPAX Database Server, log in using the AgfaService account.
2. Open a command prompt.
3. Change to the **C:\mvf\bin** directory.
4. To find out what the current sa password is, type

   passkey -M QUERY -u sa -r c:\mvf\mvf.psd
5. To update the password, type

   sqlcmd -U sa -P *password* -d master -Q "*sp_password* '*old_password*', '*new_password*', 'sa'"

   A message indicates that the password was changed.
6. To log out, type **exit**.

4. Synchronizing clocks on Windows-based IMPAX systems

(Topic number: 6752)

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

Note:

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

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

Synchronizing Windows servers to an external time source

(Topic number: 58717)

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

CAUTION!

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

To synchronize Windows servers to an external time source

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

5. To specify where the computer obtains time stamps, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer** subkey, enter the list of DNS names or IP addresses.

   If you use DNS names, append **,0x1** to the end of each DNS name.

6. To set the poll interval, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval** subkey, change the REG_DWORD value to the number of seconds between each poll.

   The recommended value is **900** Base **Decimal**, which polls the time server every 15 minutes.

7. To specify the maximum positive difference that triggers a synchronization, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection** subkey, change the REG_DWORD value to the maximum number of seconds.

   The recommended value is **3600** Base **Decimal**.

8. Similarly, to specify the maximum negative difference that triggers a synchronization, in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection** subkey, change the REG_DWORD value to the maximum number of seconds.

9. Exit the Registry Editor.

10. To stop and restart the Windows Time server, at a command prompt, type **net stop w32time && net start w32time**.

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

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

Synchronizing Windows servers to an internal time source

(Topic number: 58720)

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

CAUTION!

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

To synchronize Windows servers to an internal time source

1. To open Registry Editor, select **Start** > **Run**, type **regedit**, and click **OK**.

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

   It may take some time for this to take effect.

Note:

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

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

(Topic number: 58572)

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

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

1. Open Control Panel.
2. Select **Date and Time**.
3. Switch to the **Server Internet Time** tab.
4. In the list, type or select the time server to synchronize with.

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

(Topic number: 58569)

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

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

1. Open a command prompt.
2. Type

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

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

w32tm /config /update

4. To synchronize the clock, type

   w32tm /resync

5. 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 5.2 or 5.3 Client software

(Topic number: 51525)

IMPAX 5.2 or 5.3 Client software must be uninstalled before the IMPAX 6.5.1 Client software can be installed.

To manually uninstall the IMPAX 5.2 or 5.3 Client software

1. Open Control Panel.
2. On Windows 2003 servers, select **Add or Remove Programs**. On Windows 2008 servers, select **Programs and Features**.
3. On Windows 2003 servers, under Currently installed programs, select **IMPAX Client ES** and click **Remove**.

   or

   On Windows 2008 servers, select **IMPAX Client ES** and click **Uninstall**.
4. At the `Are you sure you want to remove this program?` prompt, click **Yes**.
5. If a Files Not Removed dialog opens, to remove the remaining files, click **Yes**.
6. At the Uninstall Successful message, click **OK**.
7. Restart the computer.
8. After the computer has restarted, verify that the C:\mvf directory has been deleted. If the directory is still present, delete it.

Removing the IMPAX 5.2 or 5.3 Client Knowledge Base

(Topic number: 58578)

If the IMPAX 5.2 or 5.3 Client Knowledge Base is installed, you must uninstall it before upgrading.

To remove the IMPAX 5.2 or 5.3 Client Knowledge Base

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

   or

   On Windows 2008 servers, click **Programs and Features**.
3. On Windows 2003 servers, select **IMPAX Client Knowledge Base 5.2** or **IMPAX Client Knowledge Base 5.3** and click **Change/Remove**.

   or

   On Windows 2008 servers, select **IMPAX Client Knowledge Base 5.2** or **IMPAX Client Knowledge Base 5.3** and click **Uninstall**.
4. In the Confirmation dialog, click **OK**.
5. If also uninstalling the IMPAX Server Knowledge Base, in the Maintenance Complete dialog, select **No, I will restart my computer later**. Otherwise, select **Yes, I want to restart my computer now** and click **Finish**.
6. If you restarted the computer, log into Windows as an administrator-level user.
7. To remove any translations of the IMPAX 5.2 or 5.3 Client Knowledge Base, delete the **C:/impax/documents/client/translations** directory.

Installing the IMPAX Client

(Topic number: 7776)

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

Note:

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

To install the IMPAX Client

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

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

6. 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.

Post-upgrade checking and stabilization

9

Some tasks are performed after the 6.5.1 upgrade is complete.

1. Installing Server license keys on an upgraded AS300 server

(Topic number: 10245)

Note:

IMPAX 5.2 and 5.3 server license key files cannot be reused with IMPAX 6.5.1 software. For information on obtaining license keys, refer to the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.

If you have not already installed the appropriate license keys on the servers, do so now. MVF license keys must be installed on each AS300 single-host and Network Gateway station. Archive license keys must be installed on each AS300 single-host and Archive Server station.

Installing the mvf license key on a Windows server

(Topic number: 40452)

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

To install the mvf license key on a Windows server

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

   The license key file name is the MAC address with a .lic file extension.

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

Installing the archive license key on a Windows server

(Topic number: 15609)

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

To install the archive license key on a Windows server

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

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

2. Testing the installed software

(Topic number: 6842)

After installing the new version of IMPAX, perform the following tests to verify that the installation was successful.

To test the installed software

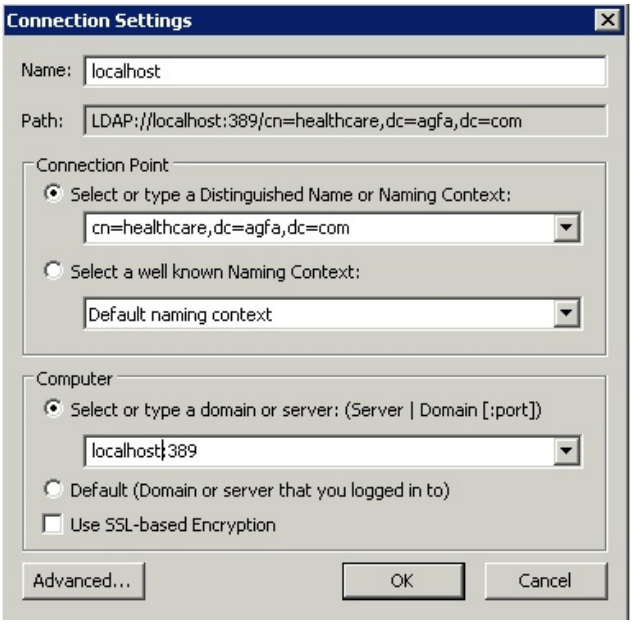
1. Ensure that the user migration was successful.
   a. On the Application Server, if Windows 2003 is the operating system, select **Start** > **All Programs** > **ADAM** and select **ADAM ADSI Edit**

      or

      On the Application Server, if Windows 2008 is the operating system, open the Windows Administrative Tools and select **ADSI Edit**.

   b. On Windows 2003, right-click **ADAM ADSI Edit** and select **Connect To**. On Windows 2008, right-click **ADSI Edit** and select **Connect To**.

   c. On the Connection Settings screen, fill in the values as shown in the following illustration.



d. To close the Connection Settings dialog, click **OK**.

e. Expand **application server node**.

f. Expand **distinguished name**.

g. Select **CN=users**.

h. Verify that the list of original IMPAX 5.2 or 5.3 migrated users is displayed.

2. Ensure that you can log into the IMPAX 6.5.1 software.

   a. On the IMPAX Database Server, run the Administration Tools and ensure that you can log in using the administration password.

   b. On the Application Server, open a web browser and connect to http://localhost. Ensure that the "Welcome to IMPAX" page is displayed.

   c. Run the IMPAX Client and ensure that you can log in using the administration password.

3. Test the status of Web Services by running a Healthcheck.

   a. Open a web browser and navigate to **http://*application_server_name*/AgfaHC.Healthcheck.Escrow/AuthenticationForm.aspx**.

   b. Log in with the administrator user and password.

3. Restarting an archive queue

(Topic number: 32239)

Restart the Archive queue or queues that were halted before the IMPAX upgrade.

To restart an archive queue

1. Log into the IMPAX 6.5.1 Administration Tools.
2. On the Daily tab, select **Job Manager**.
3. In the queue list, select the archive queue.
4. Click **Restart**.

4. 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.

5. 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*.)

6. 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.

7. Installing the PSARMT and cache tools on a Windows server

(Topic number: 40800)

For this install, you must be logged into Windows as an administrator-level user.

The PSARMT and cache tools are on the IMPAX AS300 CD. PSARMT is used with external PACS to mark studies as PACS archived. The cache check and repair tools detect and correct IMPAX cache corruption.

To install the PSARMT and cache tools on a Windows server

1. Insert the IMPAX AS300 CD.
2. Navigate to the programs\mvf directory and double-click **mvfcachecheck-6.5.0.*xx*.exe** (cache check and repair tools).
3. On the Welcome screen, click **Next**.
4. On the Setup Complete screen, click **Finish**.

   The tools are installed in the C:\mvf directory.
5. Navigate to the programs\mvf directory and double-click **mvfpsarmt-6.5.0.*xx*.exe** (PSARMT Migration Tools).
6. On the Welcome screen, click **Next**.
7. On the Setup Complete screen, click **Finish**.

The tools are installed in the C:\mvf directory.

8. Remove the IMPAX AS300 CD.

8. Running PSARMT to mark studies from an external PACS as PACS archived

(Topic number: 6629)

Note:

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 migrated IMPAX Database Server.

For more information regarding the configuration and execution of the PSARMT Migration Tools, refer to the PSARMT readme document that can be found in the C:\mvf-mig6 directory.

To run PSARMT to mark studies from an external PACS as PACS archived

1. Navigate to the C:\mvf directory.
2. Build the PSARMT database tables by running **build-mvf-psarmt-database.bat**.
3. Install the PSARMT Tools as services by running **install_psarmt.bat**.
4. Specify the migration configuration by running **mvf_psarmt_config_manager.exe**.

   Parameters are as follows:

   - **-C *configuration_file_with_all_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.

5. Start the PSARMT services by running **start_psarmt.bat**.
6. Perform the migration, based on the configuration defined in step 4, by running **mvf_psarmt.exe**.

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.exe**.

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. If you want to remove the PSARMT Tools as services, on Windows, run **remove_psarmt.bat**.

9. 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**.

10. Uninstalling the Cross-Cluster Dictation Interlock tool

(Topic number: 60390)

If you no longer have to synchronize the dictation status of studies between the 5.2 or 5.3 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 computer where the 5.2 or 5.3 Cross-Cluster Dictation Interlock components were copied, open the Windows Administrative Tools and select **Services**.
2. Right-click the **MVF Signal Relay** service and select **Stop**.
3. Close the Services window by selecting **File** > **Exit**.
4. Open a command prompt.
5. Change to the **C:\mvf\bin** directory.
6. Type

   mvf_signal_relay.exe -remove

7. Type **clui**.
8. In CLUI, type

   delete from map_ini where ini_section='signal-relay'
9. Exit CLUI by typing **exit**.
10. In Windows Explorer, navigate to C:\mvf\bin and delete the **mvf_signal_relay.exe** and the **install_relay-signal.bat** files.
11. Optionally, you can delete the **signal-relay** and **sig-relay-train** users from the IMPAX 5.2 or 5.3 Service Tools User Manager.
12. On the IMPAX 6.5.1 Application Server where the 6.5.1 Cross-Cluster Dictation Interlock components were copied, open the Windows Administrative Tools and select **Services**.
13. Right-click the **Impax Study Status Relay** service and select **Stop**.
14. Close the Services window by selecting **File** > **Exit**.
15. Open a command prompt.
16. Change to the directory containing the Cross-Cluster Dictation Interlock components—possibly C:\Program Files\Agfa\Impax Business Services.
17. Type

    uninstall_study_status_relay_service.bat.
18. Close the command prompt by typing **exit**.
19. From Windows Explorer, navigate to and delete the **study-status-signal-relay** folder (possibly from C:\Program Files\Agfa\Impax Business Service).
20. Log into an IMPAX 6.5.1 Client as an administrator user.
21. 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.

All components of the Cross-Cluster Dictation Interlock tool are now removed.

11. Stopping WEB1000 Data Currency service

(Topic number: 6755)

Important!

This topic applies only to migrations from WEB1000 systems.

Once a site is migrated to IMPAX 6.5.1, the Data Currency service between IMPAX and WEB1000 is no longer supported, so you must stop the service.

Stopping the exhibitSyncNotifier service

(Topic number: 58418)

Once a site is migrated to IMPAX 6.5.1, the exhibitSynchNotifier service is no longer supported. You must therefore stop the exhibitSyncNotifier service, if it is still running on an upgraded station.

To stop the exhibitSyncNotifier service

1. On the AS300 server, navigate to C:\mvf\sync\bin.
2. Double-click **stopExhbitSyncNotifier.bat**.

   The exhibitSyncNotifier service is stopped.

You can also uninstall Data Currency.

Uninstalling Data Currency from an AS300 server

(Topic number: 58421)

After the WEB1000 Data Currency service is stopped, you can uninstall it. To do so, you must be logged into Windowsas an administrator-level user.

To uninstall Data Currency from an AS300 server

1. Open the Windows Administrative Tools and select **Services**.
2. Locate the **Exhibit PACS Synchronization Notifier** service and stop it.
3. Exit from the Administrative Tools.
4. In Windows Explorer, navigate to the C:\mvf\sync\bin directory.
5. Run **removeSystemDate.bat**.
6. Run **removeJobQueue.bat**.
7. Run **removeSync.bat**.
8. Open Control Panel.
9. Select **Add or Remove Programs**.
10. Under Currently installed programs, select **PACS Synchronization *version***

    where *version* is the version of the software.
11. Click **Change/Remove**.
12. When prompted to confirm the removal, click **Yes**.

Data Currency is uninstalled.

12. Removing Client queues from Job Manager

(Topic number: 11640)

IMPAX 6.5.1 no longer supports cached Clients—only cacheless and standalone Clients. You must therefore remove previous Client queues, which are now obsolete, from the Job Manager.

To remove Client queues from Job Manager

1. Retrieve the AE_REF of each cached 5.2 or 5.3 Client station. In CLUI, type

   select ae_ref from map_ae where ae_title = '*DISPLAY_STATION_AE*'

2. Generate a list of cache volumes for that AE. Type

   select * from osr_volume where volume_type = 'C' and ae_ref = *ae_ref_from_step_1*

3. To check if any images exist in those caches, type

   select count(*) from osr_location where volume_ref in (*list_of_volume_refs_from_step_2*)

4. If the count in step 3 is greater than 0, to check that those images exist elsewhere in the system, type

   select location_ref from osr_location ol1 where volume_ref in (*list_of_volume_refs_from_step_2*)

   To check that the images do not exist elsewhere in the system, type

   select location_ref from osr_location ol2 where ol1.object_ref = ol2.object_ref and ol2.volume_ref not in (*list_of_volume_refs_from_step_2*)

5. If images exist elsewhere in the system, delete them from this cache. Type

   update osr_location set visible = 'F' where volume_ref in (*list_of_volume_refs_from_step_2*)

   If images appear that do not exist elsewhere in the system, stop this process and determine whether these images should exist in another cache.

6. Signal the Autopilot and wait until it finishes. Type

   signal WAKE_AUTOPILOT 0 AUTOPILOT

7. Repeat the query in step 3 and once it returns zero, delete the caches. Type

   cache remove *volume_ref*

8. Delete the services running on this AE. Type

   go service

   query

   delete *service_refs_for_AE_title*

Configuring Oracle Data Guard

A

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 112). 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 112)

     or

   - Cold backup and restore (refer to page 116)

   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 123) 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 116). 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 113).
3. For Solaris servers only: Share the Flashback area.
4. Run the Oracle Data Guard configuration on the standby server (refer to page 114).
5. Complete the Data Guard configuration on the primary server (refer to page 115).
6. Start IMPAX and the Application Server.

Running the Oracle Data Guard configuration on the primary server

(Topic number: 125049)

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

To run the Oracle Data Guard configuration on the primary server

1. Log into the primary server.

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

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

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

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

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

      Use a value as prescribed for the /flashback area by the Database Configurator tool. Do *not* include the space for the backups in this amount if backups are on their own file system. Normally, no more than two times the database size is required if backups are separated.
6. When asked if you want to continue with the RMAN backup, type **"y"**.

7. Change to the **/opt/oracle/current/dbs** (Solaris) or **C:\oracle\product\10.2.0\db_1\database** (Windows) directory.
8. On Solaris, log in as the **oracle** user and type

   mv orapw orapw.pre_dg

   orapwd file=orapw password=stayout entries=40

   On Windows, type

   mv PWDMVF.ora PWDMVF.ora.pre_dg

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

   This creates an Oracle password file.
9. To ensure that the scripts can log into SQLPlus as the sys or dbadmin user, in a command prompt, type

   sqlplus / as sysdba

   alter user sys identified by stayout;

   grant sysdba to dbadmin;

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

To start the public listener

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

Next, if using Solaris servers, share the Flashback area; otherwise go directly to restoring the database on the standby server (refer to page 114).

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 115).

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 123) 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 112) 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 117).
2. Start the public listener (refer to page 118).
3. Run the Oracle Data Guard configuration on the standby server (refer to page 118).
4. For Solaris servers only: Share the primary Flashback and database areas (refer to page 119).
5. Restore the database on the standby server (refer to page 119).
6. Complete the Data Guard configuration by linking the two servers (refer to page 122).

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 118).

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 119); otherwise, if using Windows servers, restore the database on the standby server (refer to page 119).

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 119).

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 122).

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 123) 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

Troubleshooting IMPAX B

As you upgrade IMPAX servers, you may encounter various problems.

Troubleshooting: "Finding uninstall information for the previous version of Impax" error during AS300 upgrade

(Topic number: 121194)

Issue

During an IMPAX AS300 upgrade, the following message is received:

```
Error finding uninstall information for the previous version of Impax.
Please manually uninstall.
```

Details

The IMPAX 6.5.1 installer looks for certain IMPAX 6 registry keys and, if they are not found, an error message is displayed. This may occur, for example, if an IMPAX 6.3 installation does not complete and the system is restarted. The installation needs to be manually cleaned up before IMPAX 6.5.1 can be reinstalled.

Solution

1. Manually uninstall the AS300 software.
    a. Open Control Panel.
    b. In Windows 2003, select **Add or Remove Programs**.

        or

        In Windows 2008, select **Programs and Features**.

c. Select **AGFA IMPAX AS300**.

d. Click **Change**.

e. At the prompt, type your name. Click **Next**.

f. On the Welcome screen, select **Modify**. Click **Next**.

g. Clear the checkboxes of all installed packages. Click **Next**.

h. On the Maintenance Complete screen, select **Yes, I want to restart my computer now**. Click **Finish**.

2. Log into Windows as the **AgfaService** user.
3. Delete the following registry entry if it still exists:

   `SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{787B967E-DB4F-4313-BBD7-3E2BE0AB49A5}`
4. Continue with the upgrade.

Troubleshooting: When upgrading an AS300 to IMPAX 6.5.1, the Cygwin installation hangs

(Topic number: 120883)

Issue

When upgrading an AS300 server to IMPAX 6.5.1 from a previous IMPAX version, Cygwin hangs.

Details

During an IMPAX upgrade on an AS300, Cygwin attempts to upgrade using a registry entry that may have been set incorrectly during a previous installation.

Solution

1. Cancel the Cygwin upgrade.

   Cancelling the Cygwin upgrade allows the AS300 upgrade to continue.
2. After the AS300 upgrade is complete, to verify that the Cygwin tools are working, first open a command prompt.
3. Ensure that Cygwin is in the PATH variable by entering the following:

   set PATH=%PATH%;c:\cygwin\bin
4. To test Cygwin, enter the following commands. After you enter each command, a help message is displayed.

   bash -help

   grep -help

   sed -help

   tr -help

   gawk -help

Note:

After entering one or more of these commands, you may see an error message similar to the following:

```
This application has failed to start because cygwin1.dll was not found.
Re-installing the application may fix this problem.
```

If you see an error message similar to this one, clean up the existing Cygwin installation, then re-install Cygwin as described in the following sections.

Cleaning up the existing Cygwin installation

Note:

Follow the instructions in this section only if you see an error message in response to one or more of the commands you entered in the previous section.

To clean up the existing Cygwin installation

1. Delete the c:\cygwin directory.
2. Open regedit and delete the following registry keys
   - HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions
   - HKEY_LOCAL_MACHINE\SOFTWARE\Cygwin

Re-installing Cygwin

Note:

Re-install Cygwin only after performing cleanup steps described in the previous section.

To re-install Cygwin

1. From the OracleInstall media, run setup.bat to automatically install Cygwin.
2. After the Cygwin installation is complete, use **Ctrl-c** to exit the OracleInstall installation script.

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: Some sites may notice a delay in updating clusters

(Topic number: 40944)

Issue

Cluster updates seem to take slightly longer in IMPAX 6.5.1 than they did in IMPAX 5.2 or 5.3.

Details

To boost performance at busy times, IMPAX introduces a small delay during which linked updates between multi-cluster facilities are spooled. The spooled updates can then all be performed at the same time.

If a cluster is not that busy, the 15-second delay during which updates are pooled is not ultimately beneficial, and may result in slower rather than faster cluster updates.

Solution

If the system clocks are accurate on all IMPAX core systems, you can eliminate the 15-second delay to achieve performance similar to what was available in IMPAX 5.2 and 5.3. You can do this through a SQL update to the system database.

To remove the cluster update spooling delay

1. Launch CLUI.
2. Run the following command:

   update MAP_INI set INI_VALUE = 0 where INI_SECTION = 'MVF_SCU' and INI_KEY = 'LINK_UPDATE_DELAY_TIME'

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: Reports not displaying on the IMPAX client

(Topic number: 60414)

Issue

Reports are not being displayed, and the report source is listed as UNKNOWN.

Details

This indicates a problem in the report migration.

Solution

Fixing this problems requires updates on several servers.

1. On Connectivity Manager, using ISQL, type the following:
   a. **use mcf; select distinct(issuer_of_patient_id) from mcf_patient_id where use_of_patient_id ='PRIMARY' = PrimaryDomain**
   b. **select distinct(requesting_service) from mcf_service_request = site_identifier**

      Consult Connectivity Manager support if there are multiple values for requesting_service.
2. On the Database Server, using CLUI, type the following:
   a. **select distinct(domain_id) from agfahc_patient_id = *PrimaryDomain***

      where *PrimaryDomain* matches the value used on Connectivity Manager.

      Note:

      In IMPAX, other domain_id values may exist for the global or alternate domains. Updates may be required in order to match the domain_id for the primary domain patient_ids to the Connectivity Manager's issuer_of_patient_id values for the PRIMARY use_of_patient_id.

   b. **select requesting_service from dosr_study where accession_number='xxxxxxx' = *site_identifier***

      The requesting_service value should match the Connectivity Manager site_identifier. Updates may be required in order to match the requesting_service to the Connectivity Manager requesting_service for reports associated with the specific report source.

Tip:

Use the accession_number of a study that is approved and was completed before the Broker to Connectivity Manager migration.

3. On the Application Server, using the Business Services Configuration tool:
   a. Switch to the **Web Services** tab.
   b. Under Report Information Sources, click **Add**.
   c. In the Non-Queryable RIS Report Source Provider field, type the same *site_identifier* user previously.
   d. Click **Apply**, and **OK**.
4. On the Database Server, using CLUI, type the following:

   select * from agfahc_report_access_config
5. Verify that the Report Source is configured the same as in the Application Server.
6. Set the IMPAX Client to DEBUG mode and search for **ReportQuery,QueryReport: Checking for report on**.

Troubleshooting: Unlocking the mvf user account

(Topic number: 114829)

Issue

You cannot log into SQL Server 2008 using the mvf account because the mvf user account is locked.

Details

The mvf user account gets locked if you start IMPAX immediately after upgrading to SQL Server 2008 SP1.

Solution

To unlock the mvf user account

1. Log into SQL Server 2008 using the Administrator account.
2. In the SQL Server Management Studio, open a new query window.
3. Type

   ALTER LOGIN mvf ENABLE;

   ALTER LOGIN mvf with PASSWORD = 'mvf' UNLOCK;

   GO
4. Click **Execute**.

Troubleshooting: Server name registered in SQL Server is incorrect

(Topic number: 7625)

Issue

If the server name registered in SQL Server is not the same as the server name registered in Windows, you must update the server name in SQL Server.

Details

This discrepancy may happen if you use a ghost image when installing the third-party applications.

Solution

To check the server name registered in Windows

1. Right-click **My Computer** and select **Properties**.
2. Switch to the **Computer Name** tab.

   The server name is listed as the full server name.

To check the server name registered in SQL Server

1. In a SQL Server query window, type **select @@servername**

To update the server name registered in SQL Server

1. In the SQL Server query window, type:

   sp_dropserver *old_server_name*

   go

   sp_addserver *server_name_as_in_Windows*, local

   go

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 133) mvf-clean-cache (refer to page 133), and mvf-ddo-rescue (refer to page 134), 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.

IMPAX 5.2 tables obsolete in IMPAX 6.5.1

D

Some of the entries in the IMPAX 5.2 and 5.3 database tables have become obsolete in the IMPAX 6.5.1 database.

Obsolete tables in WSQL

(Topic number: 55025)

Table name	Module name
mitra_voice_command_keywords	activex-voice
mitra_display_pinned_studies	display-sql
mitra_display_special_format	display-sql
mitra_display_config	display-sql
mitra_ae_config	display-sql
mitra_display_markup_text	display-sql
mitra_display_modality_config	display-sql
mitra_display_worklist	display-sql
mitra_user_calibration	display-sql
mitra_display_modality_toolbar	display-sql
mitra_display_hanging_protocol	display-sql

Table name	Module name
mitra_display_site_hanging	display-sql
mitra_display_toolbar_buttons	display-sql
mitra_display_format	display-sql
mitra_display_user_wizards	display-sql
mitra_display_wizards	display-sql
mitra_display_site_wizards	display-sql
mitra_display_priv_wizards	display-sql
mitra_lut_tables	display-sql
mitra_display_snapshot	display-sql
mitra_display_mpr_vr_presets	display-sql
mitra_display_ordering	display-sql
mitra_display_study_sorting	display-sql
mitra_display_xml_config	display-sql
mitra_display_wizard_state	display-sql
mitra_display_echo_values	display-sql
mitra_display_echo_data	display-sql
jselect_data_dictionary	mvf-jselect-sql
jselect_user_script_button	mvf-jselect-sql
mitra_select_available_combos	mvf-select-sql
mitra_select_available_columns	mvf-select-sql
mitra_select_user_columns	mvf-select-sql
mitra_select_user_combos	mvf-select-sql
mitra_finder_wizards	mvf-select-sql
mitra_select_toolbar	mvf-select-sql
mitra_select_user_settings	mvf-select-sql
mitra_cerner_apps	mvf-select-sql
mitra_select_telerad_aes	mvf-select-sql
mitra_select_rond_items	mvf-select-sql
mitra_select_rond_config	mvf-select-sql
mitra_select_rond_departments	mvf-select-sql

Table name	Module name
mitra_select_rond_link	mvf-select-sql
mitra_select_rond_holidays	mvf-select-sql
mitra_select_user_toolbar	mvf-select-sql
mitra_study_arrive_rule_xml	mvf-select-sql
cd_burn_wizard	mvf-select-sql
cd_export_service	mvf-select-sql
mitra_window_positions	mvf-select-sql
mitra_select_avail_context	mvf-select-sql
mitra_select_user_context	mvf-select-sql
mitra_select_status_macros	mvf-select-sql
mitra_user_enumerated_attr	mvf-select-sql
mitra_avail_study_list_columns	mvf-select-sql
mitra_user_study_list_columns	mvf-select-sql
mitra_user_study_list_defaults	mvf-select-sql
mitra_mw_finder_wizards	mvf-select-sql
mitra_user_fixup_columns	mvf-select-sql
mitra_avail_fixup_columns	mvf-select-sql
mitra_user_rond_columns	mvf-select-sql
mitra_avail_rond_columns	mvf-select-sql
dosr_user.user.data.sql	display-sql
mitra_select_user_keyword	mvf-select-sql
mitra_user_tf_report_items	mvf-select-sql
mitra_avail_tf_report_items	mvf-select-sql

Obsolete tables in ORAS

(Topic number: 55124)

Table name	Module name
mf_staff	mtk
mf_procedure	mtk

Table name	Module name
mf_location	mtk
mtk_query_constraints	mtk
mtk_user_source	mtk
mtk_user_destination	mtk
mtk_user_layout	mtk
dosr_team	dosr
dosr_user_team	dosr
dosr_user_history	dosr
dosr_password_history	dosr
dosr_privileges	dosr
dosr_wl_presets	dosr
dosr_user	dosr

External software licenses

E

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

AutoFac 2.1.13

(Topic number: 121742)

Autofac IoC Container

Copyright (c) 2007-2008 Autofac Contributors

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

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

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

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

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

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

Cygwin

(Topic number: 121758)

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

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

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

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

Preamble

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

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

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

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

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

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

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

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

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

END OF TERMS AND CONDITIONS

Editline 1.2-cstr

(Topic number: 121768)

ICU License - ICU 1.8.1 and later

(Topic number: 13533)

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.

archive

A physical device or a file system used for long-term storage and retrieval of studies.

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

backing up

The activity of copying a database to preserve it in case of a software or hardware failure.

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.

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).

I

image

A single frame taken by a modality. Certain modalities, such as a CT, MRI, or PET, take consecutive sets of images called *series*. *Studies* are combinations of series or images for a single patient.

IP address

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

J

jukebox archive

An archive with one or more drives where media is loaded, with multiple slots that hold the media for easy storage retrieval, and with a robotic changer to move media around within the jukebox.

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

mirroring

Creating backup copies of all clinical data so that damaged data can be recovered if the original is lost.

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.

MVF_SCU

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

On IMPAX systems, it runs on the Network Gateway.

N

NAS

Network Attached Storage. A storage device attached directly to a Storage Area Network (SAN) or other direct network connection.

network

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.

non-jukebox archive

Functions much like a jukebox archive, except that it has no mailslots or changer. In a non-jukebox archive configuration, a volume is considered to be offline when it leaves the drive, whereas in a jukebox configuration, the volume is considered offline when it leaves the jukebox—either via a mailslot or by manually reaching in the case and retrieving the volume.

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.

permissions, IMPAX

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

PSARMT

PACS Store and Remember Migration Tool. This tool enables a site to migrate from an external PACS system to IMPAX by allowing the external system to act as an archive server to IMPAX.

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.

standalone station

Windows server on which the IMPAX Client, AS300, and Application Server software are installed. Runs under Windows XP SP3. The standalone does not have its own installation program. To create a standalone , the AS300, Application Server, and Client installation programs are each run separately.

Index

.NET
installing Framework....98
system requirements....19
32-bit installer....60

A

accounts
Client administration....102
lockout policies, resetting....80
mvf, unlocking....131
active content enabling....38, 39
adding
SQL Server entry....71, 85
Administration Tools....102
installing package....50
Adobe Reader....12, 15, 17, 19
AgfaService user
creating account....50
password for....60
antivirus software....15, 17
starting....100
stopping....31
troubleshooting....129
Application Server
name of....22
Application Servers
connecting to SQL Server database....78
entering name of....98
hardware requirements....11
reconfiguring after upgrade....77
software requirements....12
testing installation....102
archive
clearing Logical Volume....31
installing HSM....14
installing license key....102
requirements....14
Archive Server
installing AS300 packages....72
installing licenses....101
upgrading....70
archiving studies....22, 27, 28
restarting queues....103
AS300 packages
Curator....82
installing....60
uninstalling....49, 70
upgrading....53
Audit Record Repository
configuring database connection....92
authentication....98
Autofac software license....140
automatic updates
enabling Windows....36, 37

B

backing up
cold Oracle backup....116
RMAN backup....112
SQL 2000 database....59
training server database....47, 66
upgraded database....61
Barco monitors....18, 20
browser
configuring....38, 39
requirements....12, 19
upgrading....37

C

cache check and repair tools....133
installing....105
mvf-check-cache....133
mvf-clean-cache....133

mvf-ddo-rescue....134
mvf-report-loss....134
cache migration tool....90
caches
checking DICOM objects....133
deleting location references....30
installing package....50
repairing problem files....134
reporting problem files....133
cc objects....52
CD/DVD burners....14
cdexport package installation....52
changing
default database....71, 85
SQL Server password....93
choosing
See selecting
claim status
avoiding conflicts....23
Clients
installation of....98
installing or upgrading....97
removing queues....110
testing installation....102
troubleshooting....129
uninstalling IMPAX 5.2 or 5.3....97
upgrading....90
clocks
synchronizing....94, 95, 96
closing
archive volume....28
CLUI....88
cluster linking....129
cold backups....116
linking Data Guard servers....122
comparing
snapshots....105
Compressor
package installation....52
configuring Business Services....81
configuring caches
folder permissions....87
configuring database
ODBC connection....78
Oracle Data Guard....111, 123
configuring modalities....27
configuring PAP....75
configuring Windows
configuration summary....35
DEP....57, 75
Internet Explorer....38, 39
connecting
Application Server to database....78
Audit Record Repository to database....92
components to database....71, 85
Connectivity Manager
emptying queues....24
non-queryable RIS....80
starting queues....104
stopping queues....25
control files....123
controller cards....14
copyright information....2, 140
Core package installation....50
CPU
requirements....11, 20
speed....13, 16
creating
database....60
domain user....87
report files....24, 104
server user accounts....86, 87
web caches....86
Cross-Cluster Dictation Interlock tool
running....23
uninstalling....107
Curator....52, 89
reconfiguring after upgrade....77, 82
system requirements....16
web cache....88, 89
Cygwin
installation hangs....126
Cygwin application....84
Cygwin software license....141

D

database....34
configuring Audit Record Repository connection....92
configuring connection....71, 78, 85
disabling connections to....78
installing Oracle Client....84
installing SQL Server 2008 SP1....43

marking studies as PACS archived.....106
restoring.....61
upgrading.....40, 44, 59, 63
upgrading to SQL Server 2008.....40
verifying upgrade.....45, 64
database backups
Oracle, cold.....112, 116
Database Server
replacing.....60
testing installation.....102
upgrading.....40, 59
Database Server software
upgrading.....53
database tables
obsolete.....136, 138
Data Currency service.....109
stopping.....108, 109
Data Execution Prevention (DEP)
configuring.....57, 75
Data Guard.....52, 111
configuration overview.....111
configuring RMAN backups.....123
installing package.....112
dbase partition
sharing.....119
dedicated Curator
See Curator
default packages.....72
default report source missing.....128
deleting
Client job queue.....110
log files.....32
Logical Volume.....31
portable password file.....80
references to cached images.....30
Dell server.....11, 13, 16
Dell workstation.....18
DEP
See Data Execution Prevention (DEP)
diagnostic monitor requirements.....18
dictating
avoiding conflicts.....23
directories
migrating structure for cache volumes.....90
disabling
antivirus software.....31
SQL Server connections.....78
disks
space requirements, Application Server.....11
space requirements, AS300 servers.....13, 16
documentation
giving feedback.....3
related.....10
uninstalling IMPAX 5.2.....33
uninstalling IMPAX 5.2 or 5.3...32, 33, 98
warranty statement.....2
domain
time synchronization.....96
dot NET Framework.....19, 98
downloading
Windows updates.....36, 37
DVD burners.....14

E

Editline software license.....146
emailing
documentation feedback.....3
emptying
Connectivity Manager queues.....24
queues.....29
enabling
active content.....38, 39
automatic updates.....36, 37
exhibitSyncNotifier service, stopping.....109
external PACS.....105
external software.....34
Application Server requirements.....12
client requirements.....19
IMPAX requirements.....11
licenses.....140
external time source
synchronizing to.....94

F

fixing demographic information.....27
Flashback Recovery Area
sharing.....119
Flash Recovery Area
specifying size of.....113, 117
floppy drive

Application Server.....11
AS300 servers.....13, 16
folders
cache permissions.....87
IMPAX Client.....98

G

generating
portable password file.....56, 69
getting started.....9
Ghost
backing up system with.....36, 37
system for ghosting.....132
guides
related.....10

H

halting
archive queues.....29
hard drive requirements
Application Server.....11
AS300 servers.....13, 16
Client.....18
hardware requirements.....11, 14, 18
Application Server.....11
AS300 servers.....13, 16
standalone upgrade.....20
hierarchical cache structure
migrating to.....90
HIS verification.....27
Hotfix, .NET Framework.....98
HP server.....11, 13, 16
HP workstation.....18
HSM archives.....14
installing package.....51

I

IBM server.....11, 13, 16
IE
See Internet Explorer
IMPAXoradg package.....112
ImpaxServerGroup
account.....87
adding domain user to.....87
ImpaxServerUser
account.....87
ImpaxServerUser account.....87
importing
password file.....72, 77, 80
interfaces
Connectivity Manager.....25
internal time source
synchronizing to.....95
Internet Explorer.....12, 19
configuring.....38, 39
upgrading.....37
inventory of migration.....24, 104

J

JavaScript
support.....38, 39
jobs
expediting.....29
monitoring.....26, 46, 65

K

Knowledge Bases.....38, 39
related.....10
uninstalling IMPAX.....32
uninstalling IMPAX 5.2.....33
uninstalling IMPAX 5.2 or 5.3...32, 33, 98

L

licenses
external software.....140
installing keys.....101, 102
installing with packages.....72
local Clients.....97
location
cache references.....30
logging.....32
database upgrade.....45, 64
installation activity.....53
logging in
authentication options.....98
Logical Volume, clearing.....31
loss in caches.....134

M

MAC addresses.....102
mammography monitor requirements.....18
manufacturer's responsibility.....2
marking
    studies as PACS archived.....106
McAfee software.....129
MDAC
    Application Server.....12
memory
    marking as non-executable.....57, 75
    requirements, Application Server.....11
    requirements, AS300 servers.....13, 16
    requirements, standalone upgrade.....20
migration
    supported paths.....9
Migration Tools
    database-upgrade-script.....44, 63
    migration_inventory.....24, 104
    uninstalling.....107
mirroring
    archive volume.....28
modalities
    redirecting studies.....27
modems
    Application Server.....11
    AS300 servers.....13, 16
    Client requirements.....18
module names.....136, 138
monitoring
    cache space.....86
    queues.....26, 46, 65
monitor requirements.....11, 18
MVF
    installing license.....101
    packages, installing.....50
    unlocking account.....131
mvf-check-cache.....133
mvf-clean-cache.....133
mvf-ddo-rescue.....134
mvf-report-loss.....134

N

names
    Application Server.....22
    Application Servers.....98
    AS300 Database Server.....59
    current AS300 server.....47, 66
    database.....71, 85
    SQL Server.....132
NAS usage.....87
Network Gateway.....50
    installing AS300 packages.....72
    installing licenses.....101
    upgrading.....70
network interface.....11
non-IMPAX RIS
    connecting.....80
non-queryable RIS
    connecting.....80

O

obsolete database tables.....136
    in ORAS.....138
    in WSQL.....136
OCR package.....22, 50
ODBC.....78
    configuring connection.....71, 85
OpenSSL software license.....147
operating system.....35
    requirements.....12, 15, 17, 19
    upgrades.....34
optional packages.....72
Oracle
    backing up database.....47, 66
    Client.....12, 15, 17
    Data Guard.....52, 111, 112
    installing Windows Client.....84
    uninstalling Server.....83
Oracle Data Guard
    cold backups.....116
    configuring primary server.....113, 117
    configuring standby server.....118
    restoring standby server.....114, 119
    RMAN backups.....112
ORAS database tables.....138
overview
    configuring Windows.....35
    Data Guard configuration.....111

P

packages, AS300

Curator.....82
installing on Archive Server or Network Gateway.....72
installing single-host.....60
uninstalling.....49, 70, 82
upgrading.....53
PACS Archive Provider
See PAP
PACS Store and Remember archives.....75
license for.....102
running PSARMT.....106
PAP
installing and configuring.....75
installing package.....52
passwords
AgfaService account.....50
Client administration.....102
database.....71, 85
importing file.....72, 80
portable, generating.....56, 69
portable, importing.....77
resetting policies.....80
sa account.....40
SQL Server.....78, 93
patches
Windows.....36, 37
path to cache.....86
pcAnywhere
software requirements.....15, 17
performance
cluster updates.....129
permissions
web cache folder.....87
platform
See operating system
platform requirements.....12, 19
portable password file
See passwords
post-upgrade system snapshot.....105
post-upgrade tasks.....101
preventing database inconsistencies.....30
primary database server
backing up.....113, 117
cold backup of.....116
linking to standby server.....115, 122
RMAN backup of.....112
primary volume
closing.....28
processor speeds.....20
PSARMT
installing.....105
running.....106

Q

querying
database.....28
queues
Connectivity Manager.....24, 25, 104
emptying.....29
removing.....110
restarting.....103
stopping.....26, 29

R

RAM requirements.....18
Application Server.....11
AS300 servers.....13, 16
standalone upgrade.....20
registered trademarks.....2
registering
SQL Server.....57
registry key errors
troubleshooting.....125
remote cache hosting.....87
remote Client.....97
remote PACS.....105
removing
Client job queue.....110
Cross-Cluster Dictation Interlock tool.....107
Data Currency.....108, 109
IMPAX 5.2 documentation.....33
IMPAX 5.2 or 5.3 Client software.....97
IMPAX 5.2 or 5.3 documentation.....32, 33, 98
IMPAX AS300 packages.....49, 70, 82
IMPAX documentation.....32
IMPAX Migration Tools.....107
log files.....32
PSARMT tools.....106
Windows updates.....36, 37
replacing
servers.....59

report loss for caches.....134
reports
avoiding dictation conflicts.....23
cannot open.....128
migrating.....46, 47, 65, 66
migration inventory.....24, 104
non-queryable source.....80
not showing.....130
source.....44, 63, 128
requirements
storage.....14
restarting
antivirus software.....100
archive queues.....103
queues.....104
restoring
database.....61
standby server.....114, 119
retrieving studies.....86
RIS
connecting.....80
RMAN
configuring after Data Guard.....123
RMAN backups.....112
linking Data Guard servers.....115

S

schema
upgrade.....44, 63
scripts
enabling.....38, 39
security
configuring DEP.....57, 75
folder permissions.....87
passwords.....56, 69, 93
selecting
database server name.....71, 85
time server.....94, 96
sending
jobs.....26
server
supported upgrade paths.....9
Service Pack
.NET Framework.....98
See SP2
services
Data Currency.....108, 109
stopping SQL Server.....43
Study Status Relay.....107
Service Tools.....25
setting up
See configuring
single-host servers
installing.....60
installing licenses.....101
site upgrade.....9
snapshot of system.....24, 104, 105
software requirements.....11
Application Server.....12
AS300 servers.....15, 17
Client.....19
standalone upgrade.....20
SP1
.NET Framework.....98
SQL Server.....43
SP2
Windows 2008.....35
spooling delay.....129
SQL Server
backing up database.....59
checking server name.....132
configuring the connection.....71, 85
connecting to Application Server.....78
connecting to production database.....77
disabling connections to.....78
installing package.....50
installing SP1.....43
migrating worklist and report data.....47, 66
registration, updating.....57
requirements.....15, 17
restoring database.....61
stopping services.....43
upgrading.....40
upgrading to 2008.....40
standard monitors
requirements.....11, 18
standby control file.....123
standby database server
configuring Oracle Data Guard.....118
linking to primary server.....115, 122
restoring database.....114, 119
starting

antivirus software.....100
Connectivity Manager queues.....104
PSARMT services.....106
stations.....18
status of upgrade.....45, 64
stopping
antivirus software.....31
archive queues.....29
Connectivity Manager interfaces.....25
Connectivity Manager queues.....25
SQL Server services.....43
transmit queues.....26, 46, 65
WEB1000 Data Currency service.....108, 109
storage requirements.....14
HSM.....14
storing
studies to archive.....27, 28
Stratus server.....13, 16
studies
preparing recent.....88, 89
suggestions for documentation.....3
summary
configuring Windows.....35
Data Guard configuration.....111
Symantec Ghost.....36, 37
synchronizing
server clocks.....94, 95, 96
system
requirements.....11
snapshot.....24, 104
SystemInfo.log file.....53

T

tables
database.....136, 138
tapes for backup
requirements.....13, 16
testing
connections.....71, 85
installed software.....102
SQL Server database connection.....78
times
server synchronization.....94, 95, 96
tools, Migration
database-upgrade-script.....44, 63
migration_inventory.....104
uninstalling.....107
topics in guides and Knowledge Bases
giving feedback on.....3
trademarks.....2
training server.....46, 65
backing up database.....47, 66
configuration after upgrade.....77
Curator server in.....82
migrating data from.....47, 66
redirecting modalities.....27
taking offline.....46, 65
transmit queues, stopping.....26, 46, 65
troubleshooting.....125

U

uninstall information errors
troubleshooting.....125
uninstalling
AS300 software packages.....49, 70, 82
Cross-Cluster Dictation Interlock tool.....107
Data Currency.....108, 109
IMPAX 5.2 documentation.....33
IMPAX 5.2 or 5.3 Client.....97
IMPAX 5.2 or 5.3 documentation.....32, 33, 98
IMPAX documentation.....32
IMPAX Migration Tools.....107
Oracle Client.....84
Oracle Server.....83
unknown report source.....130
unlocking
mvf user account.....131
unverified studies.....27
updating
database records.....106
name in SQL Server.....132
SQL Server registration.....57
Windows.....36, 37
upgrade problems.....45, 64
users
accounts.....131
AgfaService.....50
creating.....87
giving cache access to.....87

mvf.....61, 71, 85

V

VaultAgfa package installation.....50
verifying
server upgrade.....45, 64
video drivers
requirements.....20
volumes
closing.....28
references.....30

W

warranty statements.....2
wavelet images
making available.....88
WEB1000 Data Currency.....108, 109
web browser configuration 38
adding trusted sites.....38
enabling active content.....39
supported browsers.....12, 19
web caches.....88, 89
creating.....86
preparing.....88
Windows
authentication.....98
configuration summary.....35
configuring cache folder permissions...87
removing Oracle Server.....83
supported versions.....12, 15, 17, 19, 20
synchronizing to external time source.....94
synchronizing to internal time source..95
Time Service, configuring.....94, 96
updates.....36, 37
upgrading browser.....37
upgrading Windows 2003.....34
upgrading Windows 2008.....35
Windows Server
upgrading to 2008.....34
worklists
adding to List area.....97
migrating.....46, 47, 65, 66
workstations
requirements.....18
WSQL database tables.....136

X

Xerces C++ Parser software license.....149

Z

Zlib software license.....149