AS300 Upgrade Guide

IMPAX 6.2 or later to IMPAX 6.5.1

Upgrading the Components of an IMPAX 6.2 or later AS300 Cluster to IMPAX 6.5.1

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 177).

Giving feedback on the documentation

(Topic number: 122201)

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

To give feedback on the documentation

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

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

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

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

Contents

Getting started

1

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

Valid IMPAX upgrade paths

(Topic number: 6607)

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

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

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

Important!

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

Additional information:

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

Related documentation: IMPAX upgrades

(Topic number: 60109)

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

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

For information about using the IMPAX 6.5.1 software once it is installed, refer to the *IMPAX 6.5.1 Server Knowledge Base*, *IMPAX 6.5.1 Application Server Knowledge Base*, and *IMPAX 6.5.1 Client Knowledge Base: Extended*.

IMPAX hardware and software requirements

(Topic number: 61303)

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

IMPAX Application Server hardware and software requirements

(Topic number: 6682)

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

IMPAX Application Server: Hardware requirements

(Topic number: 6691)

The following hardware configuration is recommended for Application Servers.

Important!

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

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

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

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

IMPAX Application Server: Software requirements

(Topic number: 6621)

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

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

IMPAX AS300 Server hardware and software requirements

(Topic number: 6674)

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

IMPAX Server: Hardware requirements

(Topic number: 6690)

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

Important!

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

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

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

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

Additional AS300 hardware requirements: Storage requirements
(Topic number: 6733)

Additional hardware can be used to meet archive requirements.

IMPAX AS300 Server: Non-SCSI CD/DVD burner and controller cards
(Topic number: 58044)

OEM-supplied CD/DVD writer

IMPAX AS300 Server: HSM storage requirements
(Topic number: 6686)

Note:

Direct attached libraries are not supported in IMPAX 6.5.1.

The following HSM storage devices are supported:

- EMC
- HP
- QStar

Note:

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

IMPAX AS300 Server: Storage requirements
(Topic number: 6616)

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

IMPAX Server: External software requirements

(Topic number: 6695)

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

Component	Requirements
Operating system	**For upgrades:** Windows Server 2003 R2 SP2, Standard or Enterprise Editions, 32-bit or 64-bit (only a dedicated Database Server can be run on Windows 64-bit) or **For new installs:** Windows Server 2008 SP2, Standard or Enterprise Editions, 32-bit or 64-bit (only a dedicated Database Server can be run on Windows 64-bit)
Database software	One of the following: • Oracle 10g 32-bit Server and Client (provided on Oracle for Windows 32-bit DVD) or • Oracle 10g 64-bit Server (provided on Oracle for Windows 64-bit DVD) or • Microsoft SQL Server 2005, Standard or Enterprise Edition, with Service Pack 3 (upgrades only) or Microsoft SQL Server 2008, with Service Pack 1 (upgrades only)
Browser	Internet Explorer 8.0
Java	
Documentation	Latest version of Adobe® Reader®
Remote access (optional)	Symantec pcAnywhere version 12.5
Antivirus	McAfee Antivirus 4.5 or higher

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)
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
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.

Component	Requirements	
Other	Microsoft supported DVD RW/CDRW	
Video		
Diagnostic review workstations and high-end diagnostic review workstations	**Windows 7 (WDDM)*:** MXRT1150, 2150 MXRT5200 (covers 98% of the diagnostic requirements) MXRT7200 (high end board for IMPAX Clinical Applications such as Oasis for IMPAX) MXRT7300 (high end board for IMPAX Clinical Applications such as Oasis for IMPAX. Supported from WDDM v1.1 May/June 2010)	**Windows XP and Vista:** BarcoMed PCIe for Coronis BarcoMed PCIe for Nio BarcoMed PCIe 5MP2FH (only with monitor MF GD-5621HD) MXRT 2100/5100/7100 (not sold anymore but still supported) MXRT5200 (covers 98% of the diagnostic requirements) MXRT200 and 7300 (high-end board for IMPAX Clinical Applications such as Oasis for IMPAX)
RIS/Administrator stations and Clinical review stations	**Windows 7 (WDDM):** NVIDIA FX 1700, FX 1800, FX 4800 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

Component	Requirements
	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 6.2 or later 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 halting and emptying 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 6.2 or later upgrades: Necessary information and equipment

(Topic number: 10233)

Equipment and information for upgrading existing IMPAX 6.2 or later stations	Notes
Whether Cross-Cluster Dictation is required, for synchronizing dictation status between IMPAX 6.2, 6.3, 6.4 or 6.5, and IMPAX 6.5.1	
Windows Server 2003 R2 Service Pack 2 software (if not already installed)	

Equipment and information for upgrading existing IMPAX 6.2 or later stations	Notes
If a SQL Server site, whether to stick with SQL Server or switch to Oracle (requires Professional Services assistance)	
SQL Server 2005 SP3 software (if applicable)	
OracleInstall package for IMPAX 6.5.1 (if applicable)	
Which standard time server or source to synchronize the server clock against	
Whether using domain authentication	
Fully qualified domain name of the main Application Server	
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. Stopping data transmission to IMPAX 6.2 or later

(Topic number: 59513)

Allow remaining SEND jobs to continue until they have finished, then stop any more studies from being transmitting in the IMPAX 6.2 or later system.

To stop data transmission to IMPAX 6.2 or later

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 6.2 or later Administration 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. Archiving remaining unarchived studies

(Topic number: 7742)

Important!

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

Use the information from the latest report on archiving studies to identify remaining unarchived studies (for details, refer to the appropriate version of the *IMPAX Preparing to Upgrade Guide*). You must store these studies to the archive.

Verifying unverified studies

(Topic number: 60054)

Before archiving studies, verify all unverified studies.

To verify unverified studies

1. In the 6.2 or later Administration Tools, on the Daily tab, click **Study Manager**.
2. From the location list, select **Failed Verification**.
3. Set other search criteria to **Any** value.
4. Click **Refresh**.
5. In the search results, select all studies.
6. To fix up the studies that have failed HIS verification, click **Fix All Studies**.
7. Review the results presented in the dialog.

Storing unarchived studies

(Topic number: 58298)

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

To store unarchived studies

1. In the 6.2 or later Administration Tools, on the Daily tab, click **Study Manager**.
2. From the location list, select **Cached** (or another value that will return the unarchived studies).
3. Set other search criteria to **Any** value (or set to appropriate values).
4. Click **Refresh**.
5. In the search results, select the studies to archive.

   The Location column on the results list shows the current location of the study, and indicates which studies are only in cache (C for system cache, L for local station cache, W for web cache) and not also in an archive location (such as P for PACS archive).
6. Click **Store to Archive**.
7. To update the status of the selected studies, click **Refresh**.
8. Ensure that all studies are archived.

Note:

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

9. 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 6.2 or later Administration 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.

10. 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 6.2 or later Administration Tools, on the Daily tab, select **Job Manager**.
2. If an archive job remains in any of the queues, select the job and click **Expedite Selected Job(s)**.
3. If any other job remains in any of the queues, select the job and click **Delete selected job(s)**.

11. 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**.

12. Stopping antivirus software

(Topic number: 7616)

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

To stop antivirus software

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

13. 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 6.2 or later Administration 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.

14. 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.

15. Recording the names of previously installed IMPAX AS300 software packages

(Topic number: 29655)

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

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

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

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

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

1. On the IMPAX 6.2 or 6.3 Windows server to upgrade, select **Start** > **Run**.
2. In the Open field, type **regedit** and click **OK**.
3. In the Registry Editor, select **HKEY_LOCAL_MACHINE\SOFTWARE\Mitra Imaging Inc.** and **HKEY_LOCAL_MACHINE\SOFTWARE\Mitra** and make note of the installed packages (refer to page 173).

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 64) tasks.

If upgrading from IMPAX 6.5 to IMPAX 6.5.1, you can skip these tasks and proceed with the *Upgrading an IMPAX 6.5 Database Server to IMPAX 6.5.1* (refer to page 71) tasks.

1. Upgrading to Windows 2008

(Topic number: 107468)

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

For information regarding migration or upgrade to Windows 2008:

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

Also, consult the hardware vendor's website for information about drivers.

2. 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 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. 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 AS300 SQL Database Server to IMPAX 6.5.1

4

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).

If upgrading from IMPAX 6.5 to IMPAX 6.5.1, you can skip these tasks and proceed with the *Upgrading an IMPAX 6.5 Database Server to IMPAX 6.5.1* (refer to page 71) tasks.

If currently using an Oracle Database Server *prior* to IMPAX 6.5, you can upgrade to IMPAX 6.5.1 by proceeding with the tasks in *Upgrading an AS300 Oracle Database Server to IMPAX 6.5.1* (refer to page 48).

If wanting to convert from SQL to Oracle as part of the upgrade, contact Professional Services for assistance.

If currently using a SQL Database Server *prior* to IMPAX 6.5, you can stay with SQL Server in upgrading to IMPAX 6.5.1, as long as you upgrade to a supported version of SQL Server. Proceed with the following tasks.

Note:

Before upgrading an all-in-one server configuration (all AS300 Server and Application Server components are installed on the same computer), make sure that IIS is stopped by running **iisreset /stop** and that any Application Services are stopped including the following: IMPAX App Server Data Manager, IMPAX Audit Event Log Manager, IMPAX Dicom Object Sender, IMPAX Distributed License Manager, and IMPAX Messaging Service.

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.

Manually backing up the SQL 2000 database

(Topic number: 8858)

To guard against information loss, create backup tapes on a daily basis. In case of a major system failure, the database can be restored from a backup.

CAUTION!

If backups are not created on a regular basis, the transaction log fills up and eventually halts the operation of your system. As well, if you do not do an initial backup of your database, SQL Server assumes that you do not want transaction logs maintained.

You can use the SQL Server Enterprise Manager or the command line to perform a database backup.

Note:

Ensure that you are logged in using the AgfaService account; you cannot log into Enterprise Manager or back up the database from the command line using the Administrator account.

To manually back up the SQL 2000 database using Enterprise Manager

1. Open the SQL Server Enterprise Manager.
2. In the Explorer window of the Enterprise Manager, expand **Console Root** > **Microsoft SQL Servers** > **SQL Server Group** > ***server*** > **Databases** > ***database***

   where *server* is the name of the SQL Server that the program is running under and *database* is the name of the database to be backed up.
3. Select **Action** > **All Tasks** > **Backup database**.
4. Configure the General and Options tabs according to your preferences for items such as the type of backup, the destination, and whether to overwrite or append to the media.
5. To start the backup, click **OK**.
6. Exit the SQL Server Enterprise Manager.

To manually back up the SQL 2000 database from the command line

1. In the SQL environment, type

isql -u*user_name* -p*password* -dmaster

2. To back up the database, type

   backup database *database_name* to *device_name*

   where *database_name* is the name of the database you want to back up and *device_name* is the logical or physical name for the tape or disk device.

Upgrading SQL Server 2000 to SQL Server 2008

(Topic number: 109391)

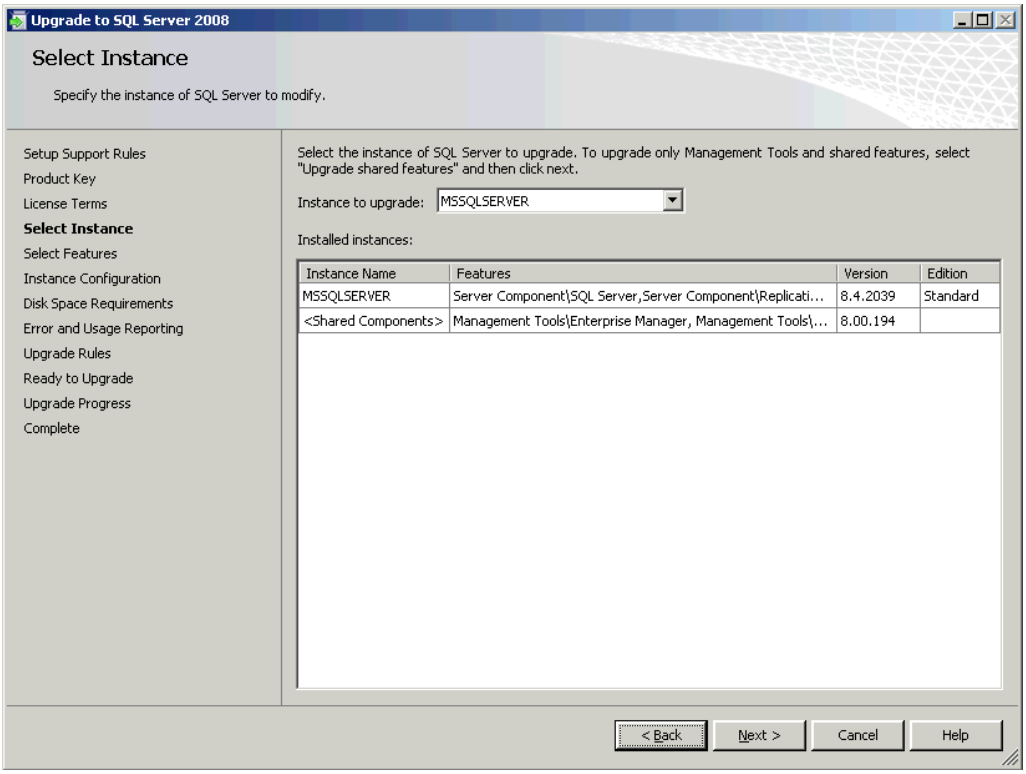
Before starting the upgrade from SQL Server 2000 to SQL Server 2008, ensure that you know the SQL Server 2000 sa database password, as you must enter it as part of the upgrade. Also ensure that you are logged into Windows as an administrator-level user.

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 167) for instructions on how to unlock the account.

2. Upgrading the IMPAX SQL Server database schema to IMPAX 6.5.1

(Topic number: 7642)

Important!

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

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

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 SQL Server database schema to IMPAX 6.5.1

1. Open a command prompt.
2. Change to the **C:\mvf-mig6\bin** directory.
3. If upgrading from IMPAX 6.5, type

   database-upgrade-script.bat

   If upgrading from IMPAX 6.2, 6.3, or 6.4, type

   database-upgrade-script.bat -v {**62** | **63** | **64**}
4. At the prompt

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

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

If the version is incorrect, type **q** and press **Enter**, then repeat the previous step with the correct version number specified.

5. If prompted for a report source, in most cases, type **UNKNOWN**.

   If using a queryable RIS and multiple Connectivity Managers, type the value used for the Connectivity Manager **issuer_of_*** and **mcf_bls_report_workflow domain_id** fields.

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

6. Respond appropriately to other prompts that appear.

The database is upgraded.

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. Upgrading an existing Database Server to IMPAX 6.5.1

(Topic number: 59510)

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).

Uninstalling the previous IMPAX software packages

(Topic number: 6744)

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

To uninstall the previous IMPAX software packages

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

   or

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

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

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 170).

Important!

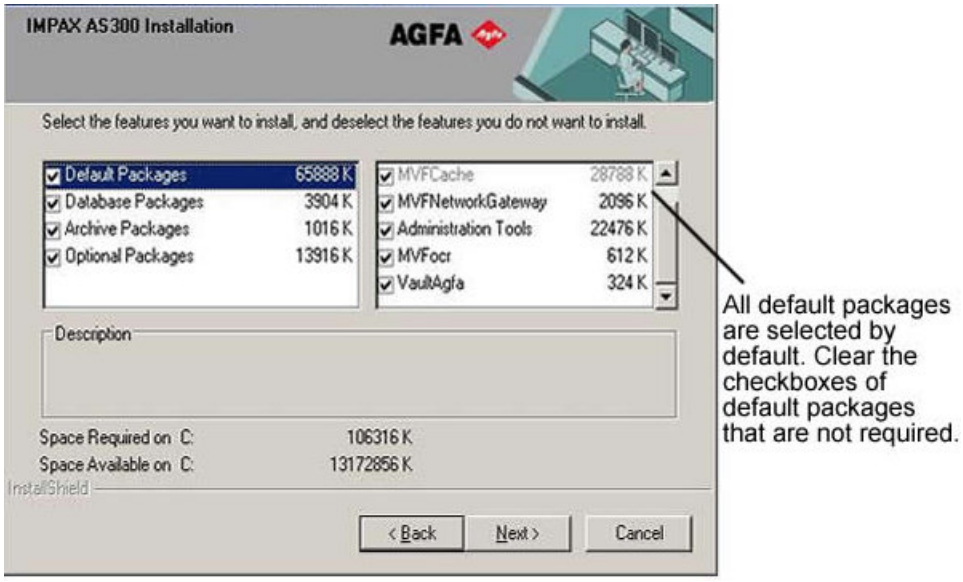
Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

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.

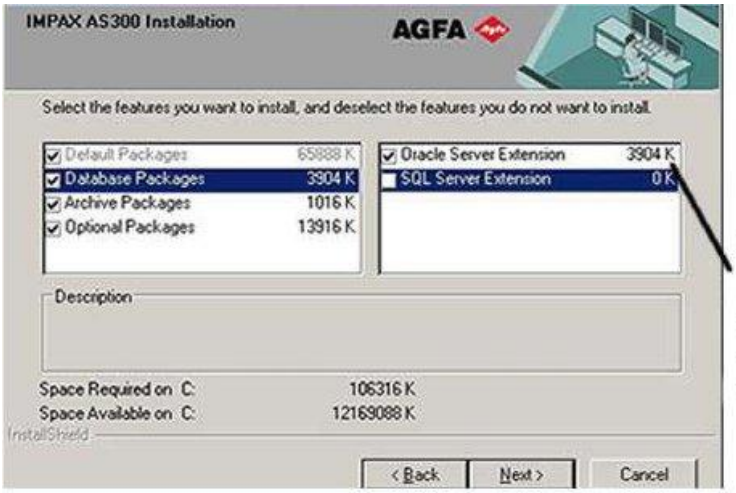
   For a single-host server, install all default packages except, potentially, the MVFocr package. For a dedicated Database Server, the MVFNetworkGateway package is not required, but can be installed.



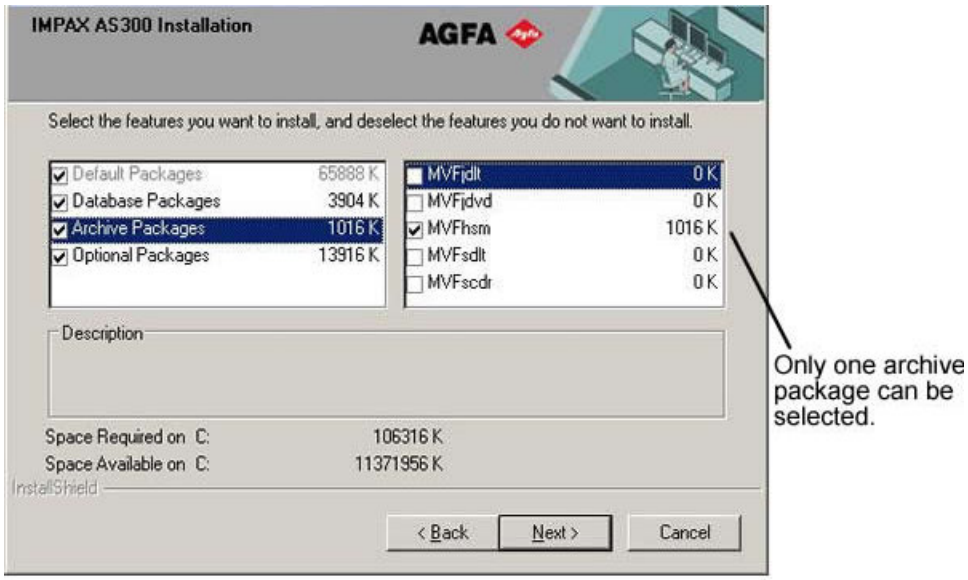
6. Select the **Database Packages** label.

   If upgrading under SQL Server, clear the **Oracle Server Extension** checkbox and select the **SQL Server Extension** checkbox.

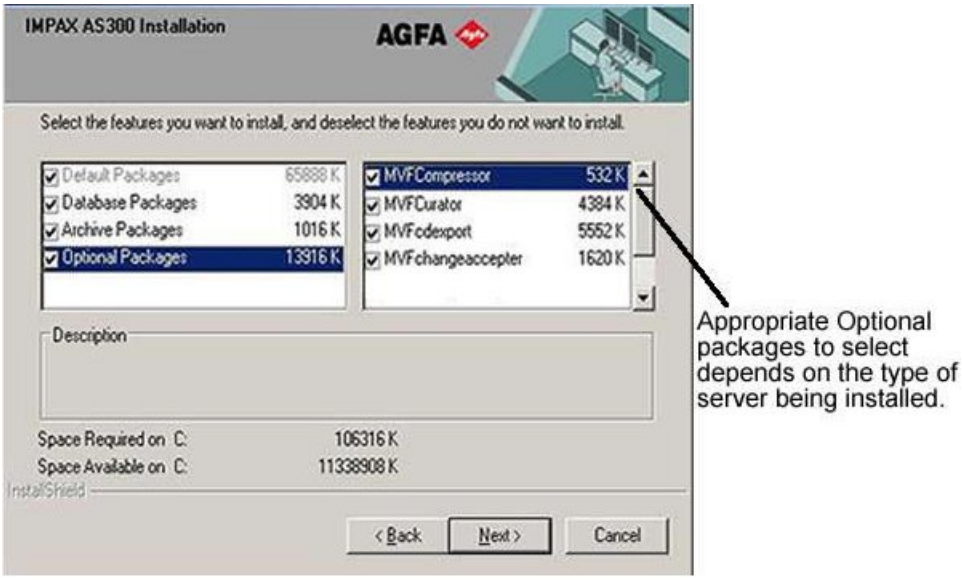
   If upgrading an IMPAX 6.4 or later Oracle Database Server, confirm that the **Oracle Server Extension** checkbox is selected.



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 .
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.

5. Generating the AS300 portable password file

(Topic number: 7694)

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

To generate the AS300 portable password file

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

   passkey -M EXPORT -k *temporary_password*

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

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

CAUTION!

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

6. 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**.

Upgrading an AS300 Oracle Database Server to IMPAX 6.5.1

5

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).

If upgrading from IMPAX 6.5 to IMPAX 6.5.1, you can skip these tasks and proceed with the *Upgrading an IMPAX 6.5 Database Server to IMPAX 6.5.1* (refer to page 71) tasks.

If currently using a SQL Database Server *prior* to IMPAX 6.5, you can upgrade to IMPAX 6.5.1 by proceeding with the tasks in *Upgrading the IMPAX SQL Server database schema to IMPAX 6.5.1* (refer to page 72).

If currently using an Oracle Database Server *prior* to IMPAX 6.5, you can upgrade to IMPAX 6.5.1 by proceeding with the following tasks.

Note:

Before upgrading an all-in-one server configuration (all AS300 Server and Application Server components are installed on the same computer), make sure that IIS is stopped by running **iisreset /stop** and that any Application Services are stopped including the following: IMPAX App Server Data Manager, IMPAX Audit Event Log Manager, IMPAX Dicom Object Sender, IMPAX Distributed License Manager, and IMPAX Messaging Service.

1. Applying patches and upgrading Oracle

(Topic number: 106570)

Note:

This topic applies only when upgrading from IMPAX 6.4 or later and to both Oracle Data Guard and non-Oracle Data Guard configurations. If you are upgrading an Oracle Data Guard cluster, the primary and standby databases can be upgraded at the same time, using the same procedure on both systems.

When upgrading an IMPAX AS300 Oracle server to IMPAX 6.5, apply the latest Oracle patches.

To apply patches and upgrade Oracle

1. Log into the Database Server as the Administrator.
2. Insert either the Oracle on Windows 32-bit DVD or the Oracle on Windows 64-bit DVD, depending on the version of Windows running on the server.
3. Open a command prompt.
4. Change to the c:\mvf-mig6\bin directory.
5. Type

   bash upgrade-oracle *location_of_DVD_drive_or_Oracle_software_repository*

   For example,

   bash upgrade-oracle d:
6. If the upgrade-oracle script aborts, it could be the due to permission problems.

   To check for permission-related errors, navigate to the c:\mvf-mig6\data\logs\upgrade-oracle.log file and search for an error similar to the following

   ```
   SEVERE:Abnormal program termination. An internal error has occured. Please
    provide the following files to Oracle Support :

   "C:\oracle\102010\Inventory\logs\installActions2010-11-09_01-49-14PM.log"
   "C:\oracle\102010\Inventory\logs\oraInstall2010-11-09_01-49-14PM.err"
   "C:\oracle\102010\Inventory\logs\oraInstall2010-11-09_01-49-14PM.out"
   ```

   If you see such an error, look in the specified .err file for the following:

   ```
   Exception java.lang.NoSuchFieldError: numFailListEntries occurred..
   java.lang.NoSuchFieldError: numFailListEntries
    at
   oracle.sysman.oii.oiip.osd.win32.OiipwWin32NativeCalls.ssntSetPermissionsw32(Native
    Method)
   ```

   If you see a similar error, the error is permission related. In this case, reset the owner. Then, open a command prompt and type **takeown /f c:\oracle /r** and run the upgrade-oracle command again.

7. At the prompt `Ready to upgrade Oracle using repository <Oracle software location>. Do you want to proceed? [y/n]`

   Verify the Oracle software location. If the location is correct, type **y** and press **Enter**.

   or

   If an Oracle Data Guard configuration is detected, you are prompted to continue the upgrade on the primary (or standby) server. Type **y** and press **Enter**.

Oracle is upgraded with the latest patches.

2. Upgrading the IMPAX Oracle database schema to IMPAX 6.5.1

(Topic number: 106573)

Run oracle-database-upgrade.bat to upgrade the IMPAX Oracle database schema to IMPAX 6.5.1. On Oracle Data Guard systems, this procedure has to be done on the primary database only.

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 Oracle database schema to IMPAX 6.5.1

1. Open a command prompt.
2. Change to the C:\mvf-mig6\bin directory.
3. Type

   oracle-database-upgrade.bat

4. At the prompt `Ready to upgrade database. Do you want to proceed [y,n]?`, type **y** and press **Enter**.

The database is upgraded.

3. Checking the status of Oracle upgrades

(Topic number: 110410)

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 Oracle upgrades

1. Navigate to the C:\mvf-mig6\data\logs directory.
2. Open the **database_upgrade.log** file.
3. Ensure that `Migration Complete Successful` appears at the end of the log file.
4. 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. Upgrading an existing Database Server to IMPAX 6.5.1

(Topic number: 59510)

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).

Uninstalling the previous IMPAX software packages

(Topic number: 6744)

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

To uninstall the previous IMPAX software packages

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

   or

   For uninstalling IMPAX 6.4 and later, click **Remove**.

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

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

Upgrading the IMPAX AS300 32-bit or 64-bit Oracle Data Guard Database Server software

(Topic number: 119131)

Important!

This topic applies only when upgrading an existing Oracle Data Guard Database Server. To upgrade a non-Oracle Data Guard Database Server, skip this procedure and proceed with *Upgrading the IMPAX AS300 32-bit Database Server software* (refer to page 78).

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. Descriptions of the packages are available in *32-bit AS300 installer packages reference* (refer to page 170) and *64-bit AS300 installer packages reference* (refer to page 172).

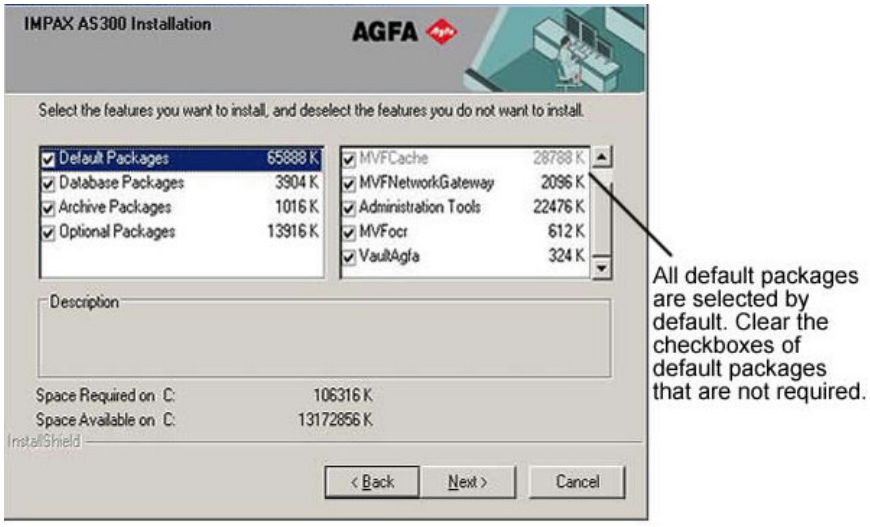
Important!

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 or 64-bit Oracle Data Guard Database Server software

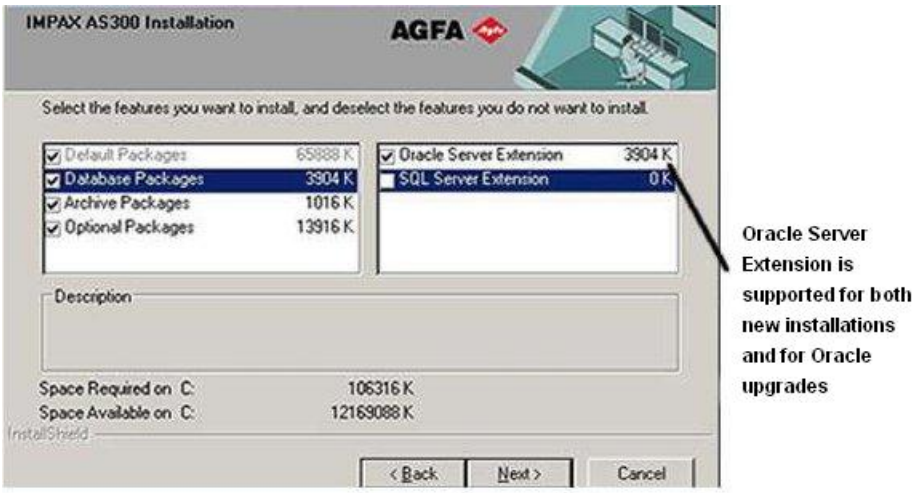
1. Insert the IMPAX AS300 DVD.
2. Navigate to D:\programs\mvf and double-click **as300-installer.exe**.
3. Type your name (minimum three characters).

   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 **MVFNetworkGateway** checkbox and any other packages that are not required.



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

   Confirm that the **Oracle Server Extension** checkbox is selected.



7. Clear the **Archive Packages** checkbox.
8. Select the **Optional Packages** label, then select the **MVForadg** checkbox. All other checkboxes should be cleared.
9. Click **Next**.
10. When prompted, type the password for the AgfaService user.

    The password must follow the requirements outlined in .
11. To confirm that the database is compatible, click **Yes**.
12. On the Ready to begin installation screen, click **Next**.

    The files are copied to the system.
13. To display the log file for the database scripts, when prompted, click **Yes**.
14. Check the log files for errors, then close the log files.

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

15. 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.

16. When the computer restarts, log into Windows as an administrator-level user.
17. On both the primary and standby servers, restore the following files:

    C:\oracle\product\10.2.0\db_1\NETWORK\ADMIN\listener.ora.dg65

    C:\oracle\product\10.2.0\db_1\NETWORK\ADMIN\tnsnames.ora.dg65

    IMPAX renames the existing tnsnames.ora file to tnsnames.dg65 and creates an updated tnsnames.ora; it does the same for listener.ora.

18. Rename the new tnsnames.ora to **tnsnames.ora.new**, then restore the **tnsnames.ora** and the **listener.ora** files.

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 170).

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).

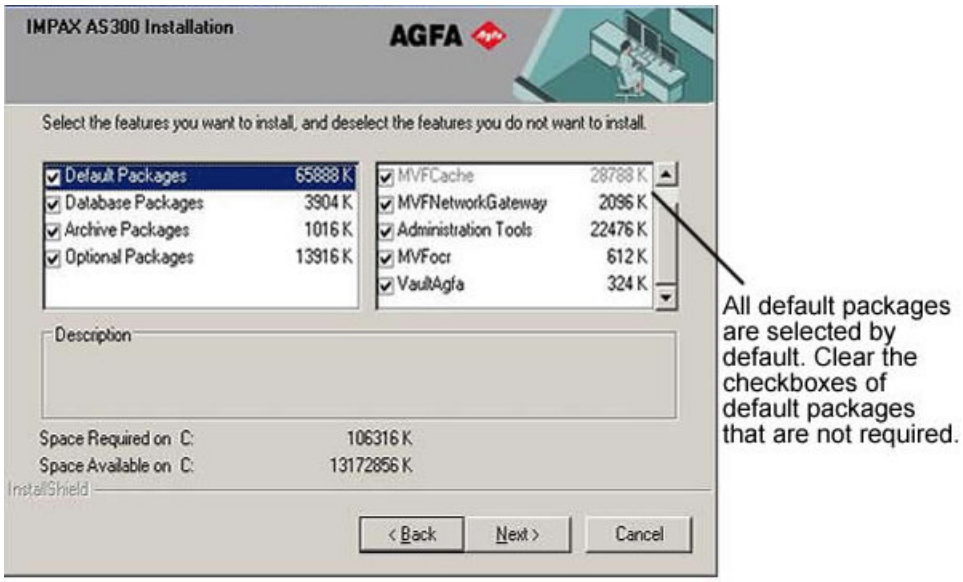
To upgrade the IMPAX AS300 32-bit Database Server software

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.

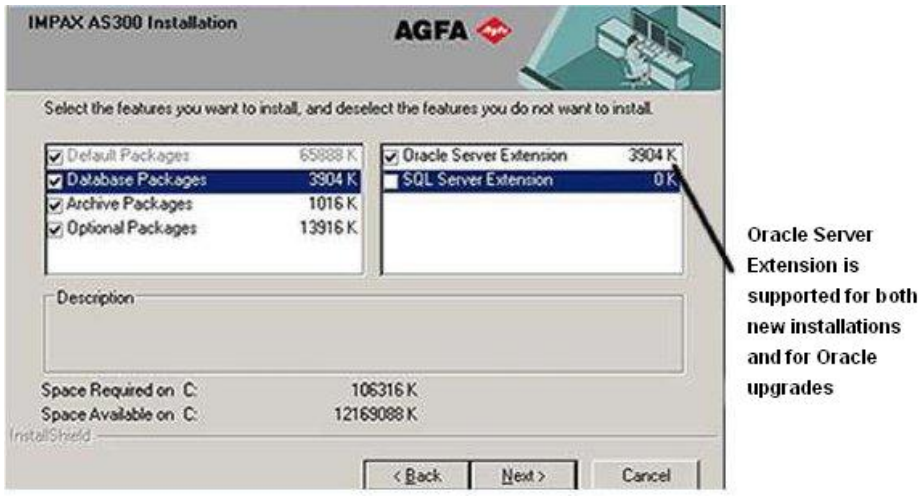
For a single-host server, install all default packages except, potentially, the MVFocr package. For a dedicated Database Server, the MVFNetworkGateway package is not required, but can be installed.



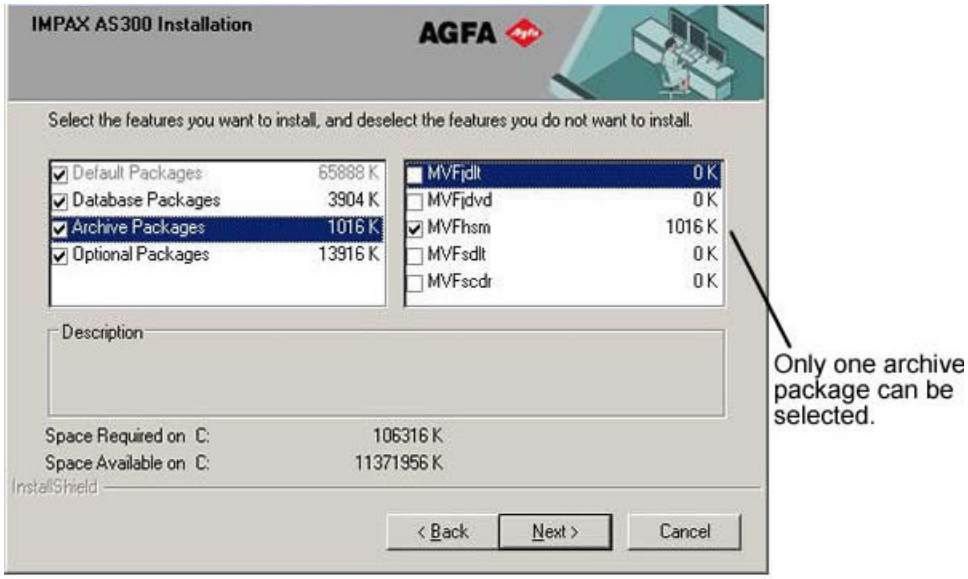
6. Select the **Database Packages** label.

   If upgrading under SQL Server, clear the **Oracle Server Extension** checkbox and select the **SQL Server Extension** checkbox.

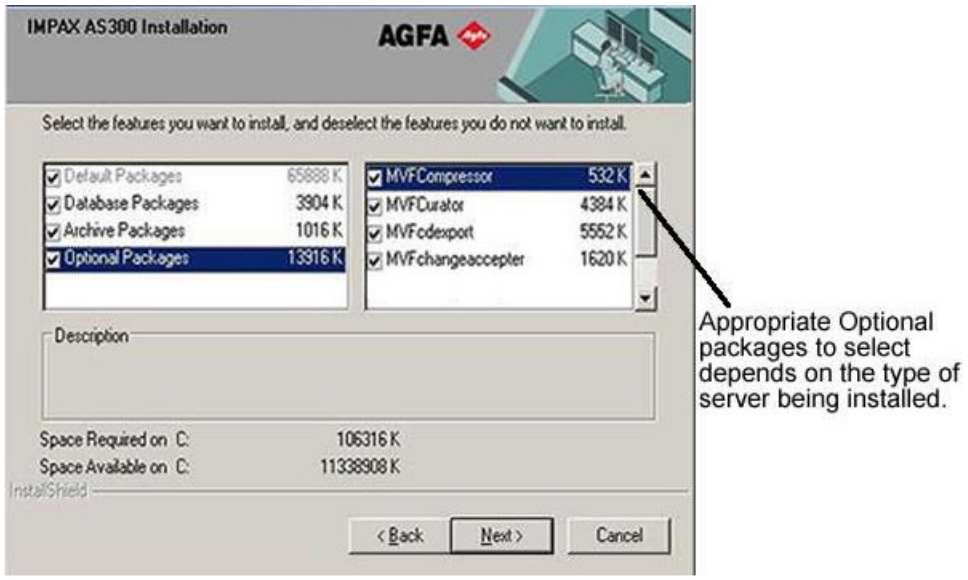
   If upgrading an IMPAX 6.4 or later Oracle Database Server, confirm that the **Oracle Server Extension** checkbox is selected.



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 .

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.

Upgrading a dedicated 64-bit IMPAX AS300 Database Server

(Topic number: 113670)

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

Note:

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

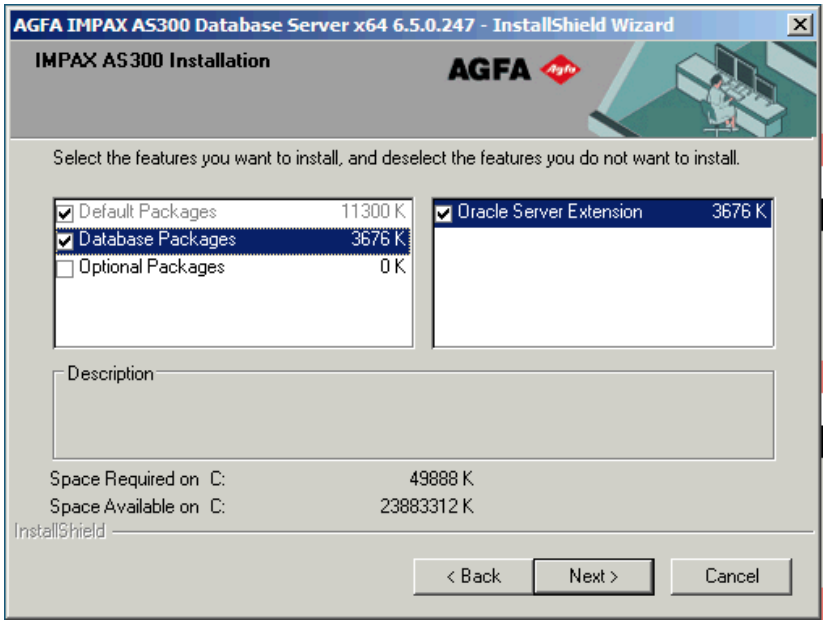
To upgrade an IMPAX AS300 Server, you must be logged into Windows as an administrator-level user.

To upgrade a dedicated 64-bit IMPAX AS300 Database Server

1. Insert the IMPAX AS300 DVD.
2. Navigate to **D:\programs\mvf** and double-click **as300-installer-64.exe**.
3. Type your name (minimum three characters).

    This information is recorded in the installer log file.

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



6. On the Type of Install screen, select **Use an existing database** and click **Next**.
7. Click **Install**.
8. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

5. Generating the AS300 portable password file

(Topic number: 7694)

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

To generate the AS300 portable password file

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

   passkey -M EXPORT -k *temporary_password*

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

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

CAUTION!

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

6. Installing the recommended version of the Oracle Client

(Topic number: 106750)

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

Important!

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

Determining the version of the installed Oracle Client

(Topic number: 106578)

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

Important!

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

To determine the version of the installed Oracle Client

1. Open a command prompt.
2. Type

   sqlplus -V

If the command returns `SQL*Plus: Release 10.2.0.1.0 - Production`, version 10.2.0.1 is installed and needs to be uninstalled first. For further details, see *Removing ODBC entries prior to uninstalling the Oracle Client* (refer to page 101) and *Uninstalling the previous version of Oracle Client* (refer to page 101)

If the command returns `SQL*Plus: Release 10.2.0.4.0 - Production`, version 10.2.0.4 is installed and needs to be upgraded. For further details, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 105).

Uninstalling the previous version of Oracle Client

(Topic number: 65367)

CAUTION!

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

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

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

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

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

To uninstall the previous version of Oracle Client

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

4. Click **Remove**.

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

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

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

Installing and configuring the Oracle 10g Client for Windows

(Topic number: 6790)

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

Determine which Oracle Client is installed on the system; see *Determining the version of the installed Oracle Client* (refer to page 100). If Oracle Client version 10.2.0.1 is installed, uninstall it. If Oracle Client version 10.2.0.4 is installed, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 105).

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

Important!

Before installing the Oracle Client, disable virus protection software.

To install and configure the Oracle 10g Client for Windows

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

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

7. At the `Where is the temporary work directory? [ C:\cygwin\temp] ?` prompt, click **Enter** to accept the default location. Otherwise, type the directory to use.

   A series of messages appears as Oracle is installed and configured.

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

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

Note:

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

Upgrading to the 10.2.0.4 version of the Oracle Client for Windows

(Topic number: 106600)

Important!

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

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

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

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

   For example, **bash upgrade-oracle d:**

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

The Oracle Client is upgraded.

Reconfiguring ODBC data source names

(Topic number: 67665)

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

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

To reconfigure ODBC data source names

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

   where *Oracle_instance_name* is the name typed when *Installing and configuring the Oracle 10g Client for Windows* (refer to page 102).
6. Click **Finish**.
7. In the Data Source Name field, type **mvf**.
8. Type a description, if needed.
9. In the TNS Service Name field, type **MVF.world**.
10. In the User Name field, type **mvf**.

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

Replacing an existing Database Server with a new station

6

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 6.2 or later 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 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. Manually backing up the SQL database

(Topic number: 7635)

Note:

Before backing up the database confirm that you have stopped the IMPAX services, emptied and halted all queues, and shut the database down.

Ensure that you are logged in using the AgfaService account; you cannot log into SQL Server Management Studio or back up the database from the command line using the Administrator account.

This procedure applies to SQL Server 2005 and SQL Server 2008.

To guard against information loss, back up the database information to 4 mm tapes or disk daily. In case of system failure, the database can then be restored from the copy.

CAUTION!

If backups are not created on a regular basis, the transaction log fills up and eventually halts the operation of your system. As well, if you do not do an initial manual backup of your database, SQL Server assumes that you do not want transaction logs maintained. If using a tape backup, to ensure that you have up-to-date backups and backups in reserve, change the tape daily.

To manually back up the SQL database using SQL Server Management Studio

1. Select **Start** > **All Programs** > **Microsoft SQL Server**.
2. Right-click **SQL Server Management Studio** and select **Run as**.
3. Select **The following user**. Type **AgfaService** as the user name, and the AgfaService password.

   If you do not know the AgfaService password, you can run the passkey utility to find it: **passkey -M QUERY -u AgfaService**.
4. In the Object Explorer window, expand ***server*** > **Databases** > ***database_name***

   where *server* is the name of the SQL Server that IMPAX is running under and *database_name* is the name of the database to be backed up.
5. Right-click ***database_name*** and select **Tasks** > **Backup**.

6. Configure the General and Options tabs according to your preferences for items such as the type of backup, the destination, and whether to overwrite or append to the media.
7. To start the backup, click **OK**.
8. Exit the SQL Server Management Studio.

To manually back up the SQL database from the command line

1. At a command prompt, type

   sqlcmd -U sa -P *sa_password* -dmaster
2. To back up the database, type

   backup database *database_name* to *device_name*

   where *database_name* is the name of the database to back up and *device_name* is the logical or physical name of the tape or disk device.

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 SQL Server database schema to IMPAX 6.5.1

(Topic number: 7642)

Important!

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

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

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 SQL Server database schema to IMPAX 6.5.1

1. Open a command prompt.
2. Change to the **C:\mvf-mig6\bin** directory.
3. If upgrading from IMPAX 6.5, type

   database-upgrade-script.bat

   If upgrading from IMPAX 6.2, 6.3, or 6.4, type

   database-upgrade-script.bat -v {**62** | **63** | **64**}
4. At the prompt

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

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

   If the version is incorrect, type **q** and press **Enter**, then repeat the previous step with the correct version number specified.
5. If prompted for a report source, in most cases, type **UNKNOWN**.

   If using a queryable RIS and multiple Connectivity Managers, type the value used for the Connectivity Manager **issuer_of_*** and **mcf_bls_report_workflow domain_id** fields.

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

6. Respond appropriately to other prompts that appear.

The database is upgraded.

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. 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 an IMPAX 6.5 Database Server to IMPAX 6.5.1

7

These tasks apply only when upgrading an IMPAX Database Server already on IMPAX 6.5.

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).

If currently using a SQL Database Server *prior* to IMPAX 6.5, you can upgrade to IMPAX 6.5.1 by following the tasks in *Upgrading the IMPAX SQL Server database schema to IMPAX 6.5.1* (refer to page 72).

If currently using an Oracle Database Server *prior* to IMPAX 6.5, you can upgrade to IMPAX 6.5.1 by following the tasks in *Upgrading the IMPAX Oracle database schema to IMPAX 6.5.1* (refer to page 74).

Note:

Before upgrading an all-in-one server configuration (all AS300 Server and Application Server components are installed on the same computer), make sure that IIS is stopped by running **iisreset /stop** and that any Application Services are stopped including the following: IMPAX App Server Data Manager, IMPAX Audit Event Log Manager, IMPAX Dicom Object Sender, IMPAX Distributed License Manager, and IMPAX Messaging Service.

1. Overview of upgrading an IMPAX 6.5 Database Server to IMPAX 6.5.1

(Topic number: 126839)

If the existing IMPAX 6.5 Database Server has an adequate hardware profile, you can upgrade it to IMPAX 6.5.1, saving on the cost of new hardware. Follow these steps:

1. Upgrade the SQL Server database schema (refer to page 72) and then check the status of the upgrade (refer to page 73).

   or

   Upgrade the Oracle database schema (refer to page 74) and then check the status of the upgrade (refer to page 74).
2. Uninstall the previous IMPAX software package.
3. Upgrade the IMPAX Oracle Data Guard Database Server software (refer to page 75).

   or

   Upgrade the IMPAX AS300 32-bit Database Server software (refer to page 78).

   or

   Upgrade a dedicated 64-bit IMPAX AS300 Database Server (refer to page 81).

2. Upgrading the IMPAX SQL Server database schema to IMPAX 6.5.1

(Topic number: 7642)

Important!

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

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

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 SQL Server database schema to IMPAX 6.5.1

1. Open a command prompt.
2. Change to the **C:\mvf-mig6\bin** directory.
3. If upgrading from IMPAX 6.5, type

   database-upgrade-script.bat

   If upgrading from IMPAX 6.2, 6.3, or 6.4, type

   database-upgrade-script.bat -v {**62 | 63 | 64**}
4. At the prompt

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

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

   If the version is incorrect, type **q** and press **Enter**, then repeat the previous step with the correct version number specified.
5. If prompted for a report source, in most cases, type **UNKNOWN**.

   If using a queryable RIS and multiple Connectivity Managers, type the value used for the Connectivity Manager **issuer_of_*** and **mcf_bls_report_workflow domain_id** fields.

   This value is the facility sending name entered in the HL7 In field in Connectivity Manager Service Tools when mapping report sources.
6. Respond appropriately to other prompts that appear.

The database is upgraded.

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.

3. Upgrading the IMPAX Oracle database schema to IMPAX 6.5.1

(Topic number: 106573)

Run oracle-database-upgrade.bat to upgrade the IMPAX Oracle database schema to IMPAX 6.5.1. On Oracle Data Guard systems, this procedure has to be done on the primary database only.

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 Oracle database schema to IMPAX 6.5.1

1. Open a command prompt.
2. Change to the C:\mvf-mig6\bin directory.
3. Type

   oracle-database-upgrade.bat

4. At the prompt `Ready to upgrade database. Do you want to proceed [y,n]?`, type **y** and press **Enter**.

The database is upgraded.

Checking the status of Oracle upgrades

(Topic number: 110410)

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 Oracle upgrades

1. Navigate to the C:\mvf-mig6\data\logs directory.

2. Open the **database_upgrade.log** file.
3. Ensure that `Migration Complete Successful` appears at the end of the log file.
4. 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. Uninstalling the previous IMPAX software packages

(Topic number: 6744)

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

To uninstall the previous IMPAX software packages

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

   or

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

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

5. Upgrading the IMPAX AS300 32-bit or 64-bit Oracle Data Guard Database Server software

(Topic number: 119131)

Important!

This topic applies only when upgrading an existing Oracle Data Guard Database Server. To upgrade a non-Oracle Data Guard Database Server, skip this procedure and proceed with *Upgrading the IMPAX AS300 32-bit Database Server software* (refer to page 78).

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. Descriptions of the packages are available in *32-bit AS300 installer packages reference* (refer to page 170) and *64-bit AS300 installer packages reference* (refer to page 172).

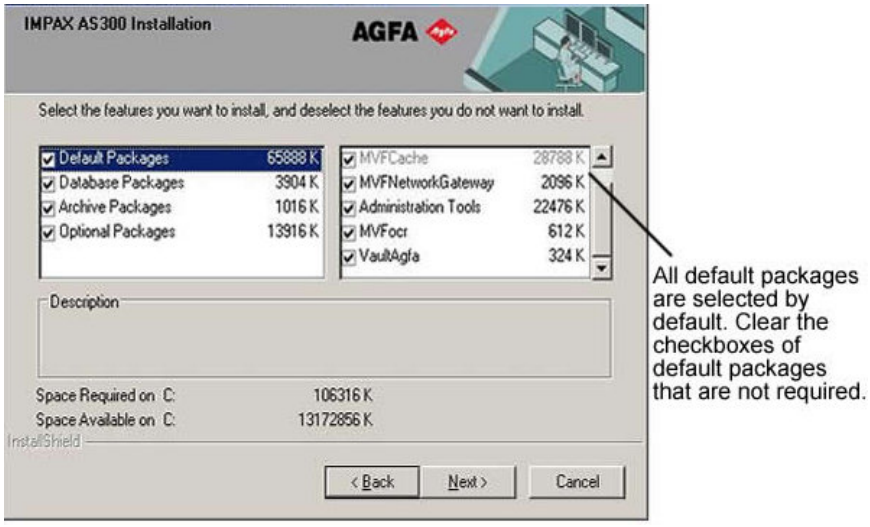
Important!

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 or 64-bit Oracle Data Guard Database Server software

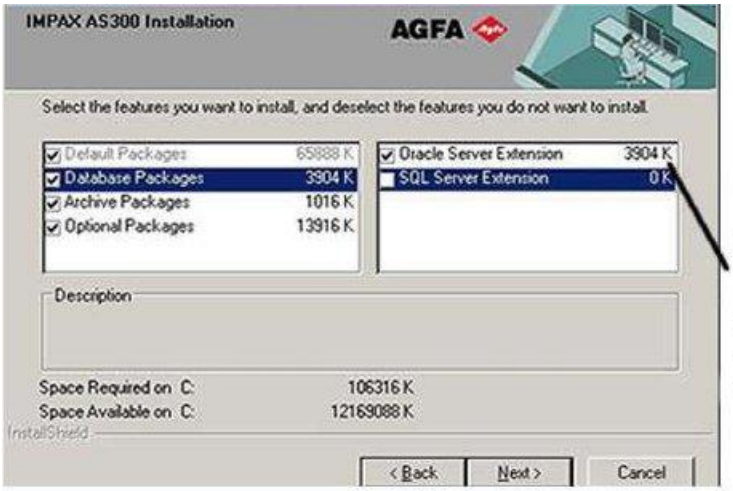
1. Insert the IMPAX AS300 DVD.
2. Navigate to D:\programs\mvf and double-click **as300-installer.exe**.
3. Type your name (minimum three characters).

   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 **MVFNetworkGateway** checkbox and any other packages that are not required.



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

   Confirm that the **Oracle Server Extension** checkbox is selected.



7. Clear the **Archive Packages** checkbox.
8. Select the **Optional Packages** label, then select the **MVForadg** checkbox. All other checkboxes should be cleared.
9. Click **Next**.
10. When prompted, type the password for the AgfaService user.

    The password must follow the requirements outlined in .
11. To confirm that the database is compatible, click **Yes**.
12. On the Ready to begin installation screen, click **Next**.

    The files are copied to the system.
13. To display the log file for the database scripts, when prompted, click **Yes**.
14. Check the log files for errors, then close the log files.

    The log files must be closed for the installation script to continue.
15. 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.
16. When the computer restarts, log into Windows as an administrator-level user.
17. On both the primary and standby servers, restore the following files:

    C:\oracle\product\10.2.0\db_1\NETWORK\ADMIN\listener.ora.dg65

    C:\oracle\product\10.2.0\db_1\NETWORK\ADMIN\tnsnames.ora.dg65

    IMPAX renames the existing tnsnames.ora file to tnsnames.dg65 and creates an updated tnsnames.ora; it does the same for listener.ora.
18. Rename the new tnsnames.ora to **tnsnames.ora.new**, then restore the **tnsnames.ora** and the **listener.ora** files.

6. 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 170).

Important!

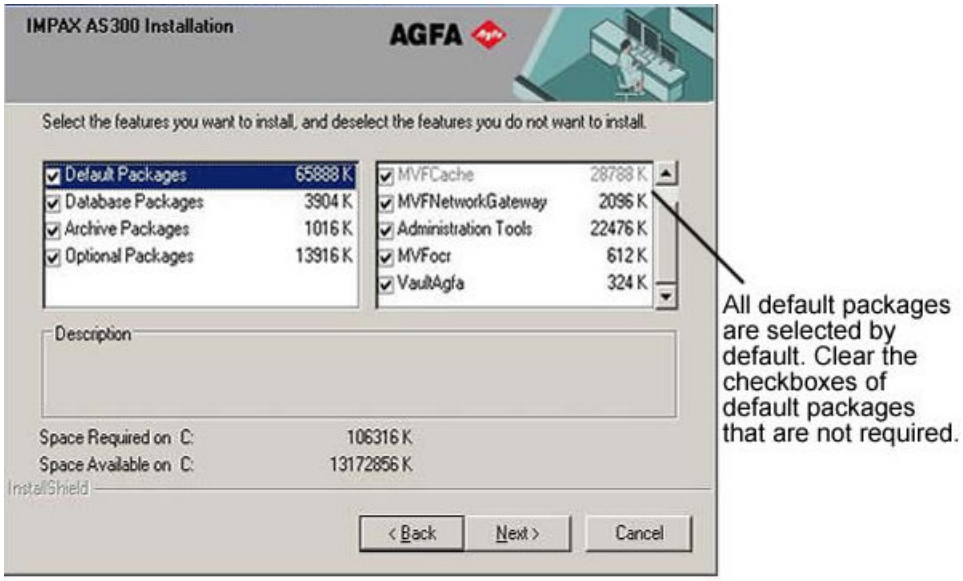
Only specific IMPAX upgrade paths are supported, and it may not be possible to upgrade certain versions or SUs. More information is provided in *Valid IMPAX upgrade paths* (refer to page 9).

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.

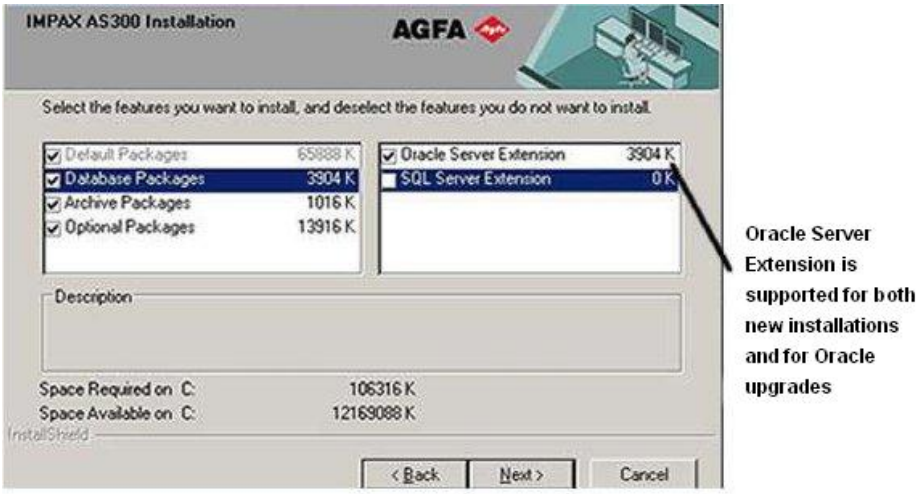
   For a single-host server, install all default packages except, potentially, the MVFocr package. For a dedicated Database Server, the MVFNetworkGateway package is not required, but can be installed.



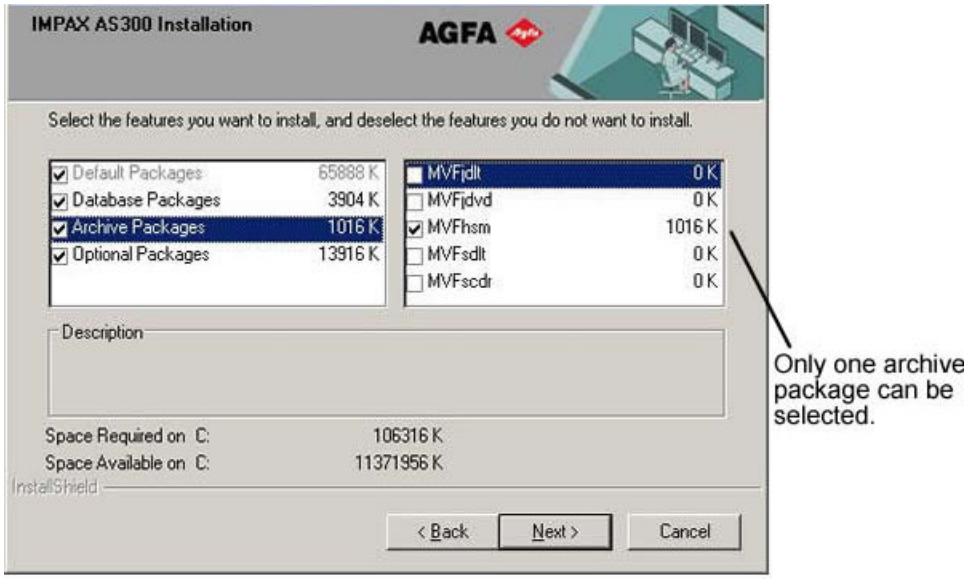
6. Select the **Database Packages** label.

   If upgrading under SQL Server, clear the **Oracle Server Extension** checkbox and select the **SQL Server Extension** checkbox.

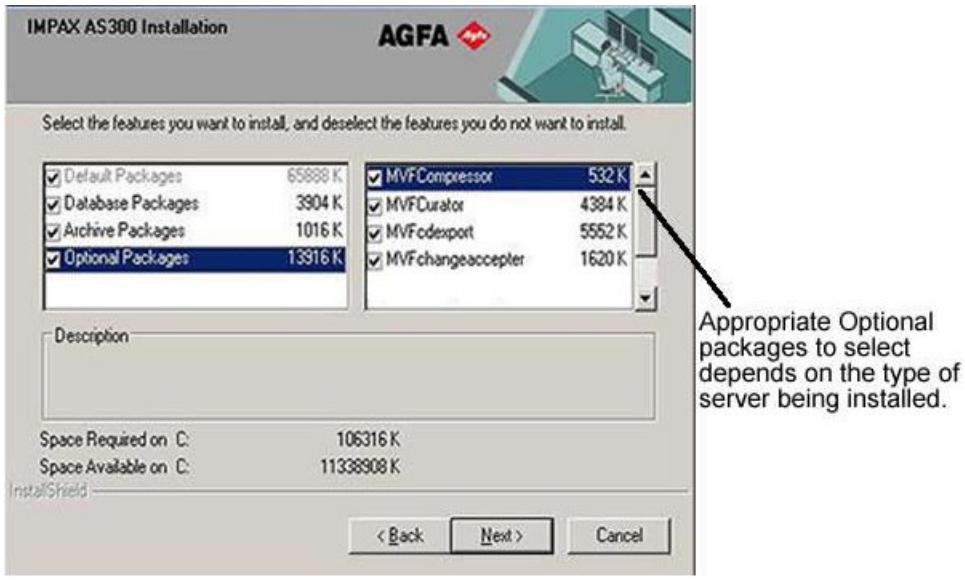
   If upgrading an IMPAX 6.4 or later Oracle Database Server, confirm that the **Oracle Server Extension** checkbox is selected.



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 .

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.

7. Upgrading a dedicated 64-bit IMPAX AS300 Database Server

(Topic number: 113670)

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

Note:

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

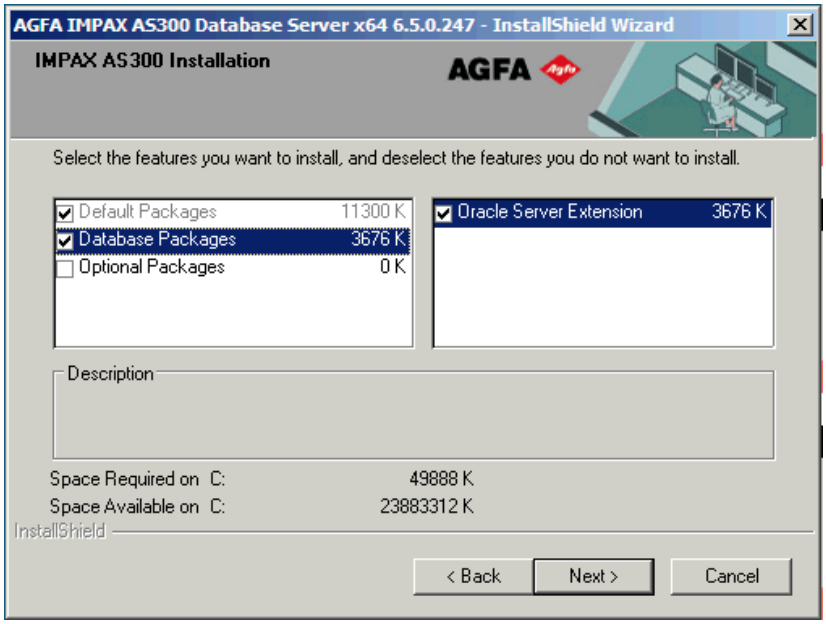
To upgrade an IMPAX AS300 Server, you must be logged into Windows as an administrator-level user.

To upgrade a dedicated 64-bit IMPAX AS300 Database Server

1. Insert the IMPAX AS300 DVD.
2. Navigate to **D:\programs\mvf** and double-click **as300-installer-64.exe**.
3. Type your name (minimum three characters).

   This information is recorded in the installer log file.

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



6. On the Type of Install screen, select **Use an existing database** and click **Next**.
7. Click **Install**.
8. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

Upgrading other AS300 servers to IMPAX 6.5.1

8

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, Network Gateway, or Curator server 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, Archive Server, and Curator 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 6.2 *version***, **Agfa IMPAX 6.3 *version***, or **Agfa IMPAX AS300** (used for IMPAX 6.4 and later).
4. Click **Change/Remove**.

   or

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

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

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 170).

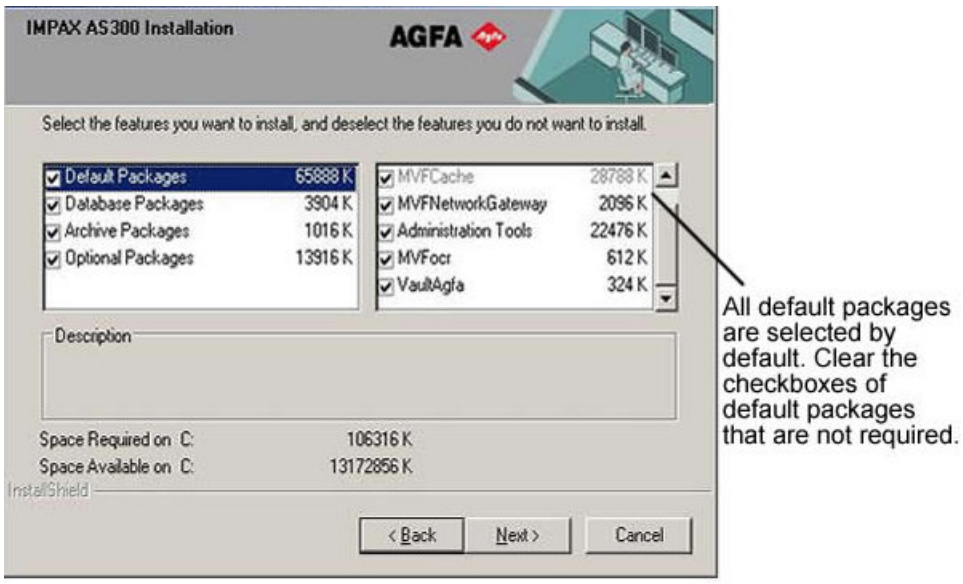
To install the IMPAX 6.5.1 AS300 Network Gateway and Archive Server packages

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.

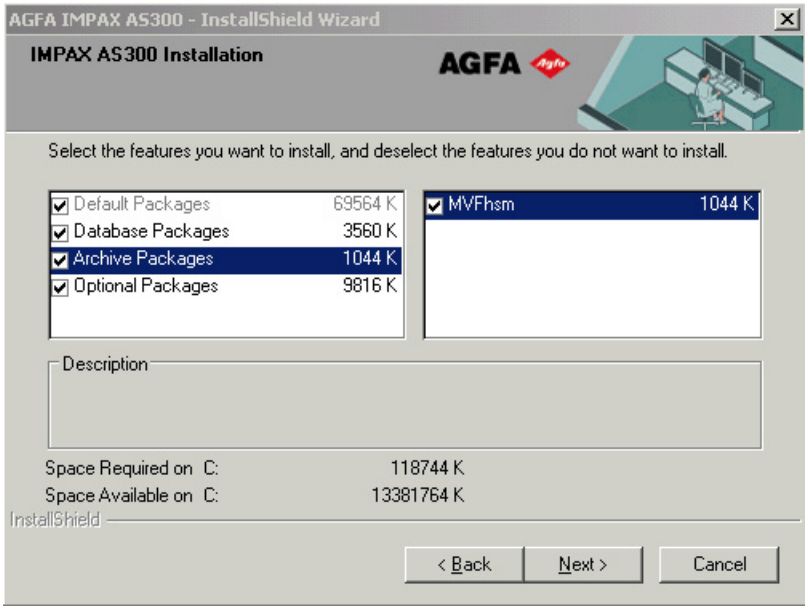
   If installing a Network Gateway or an Archive Server/Network Gateway combination, you can normally leave all the default packages selected.

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

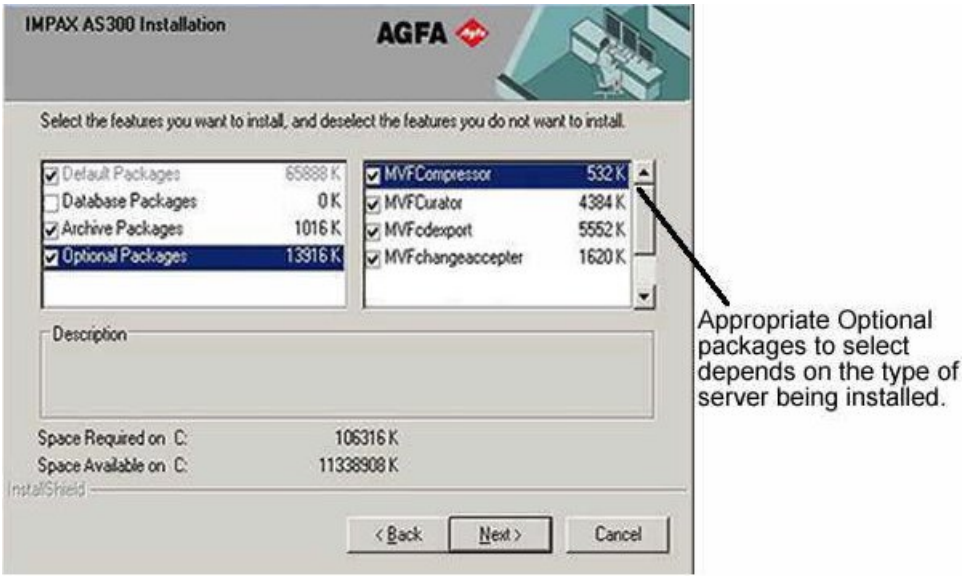


6. Clear the **Database Packages** checkbox.
7. For Archive Servers, select the **Archive Package** label. The MVFhsm is the only archive package listed and is selected by default. If not using an HSM archive, clear the **MVFhsm** checkbox; otherwise, keep it selected.

   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. Upgrading the Curator

(Topic number: 59657)

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

Uninstalling the previous IMPAX software packages

(Topic number: 6744)

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

To uninstall the previous IMPAX software packages

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

3. Under Currently installed programs, select **Agfa IMPAX 6.2 *version***, **Agfa IMPAX 6.3 *version***, or **Agfa IMPAX AS300** (used for IMPAX 6.4 and later).
4. Click **Change/Remove**.

   or

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

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

Installing the Curator and CD Export server software

(Topic number: 7047)

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

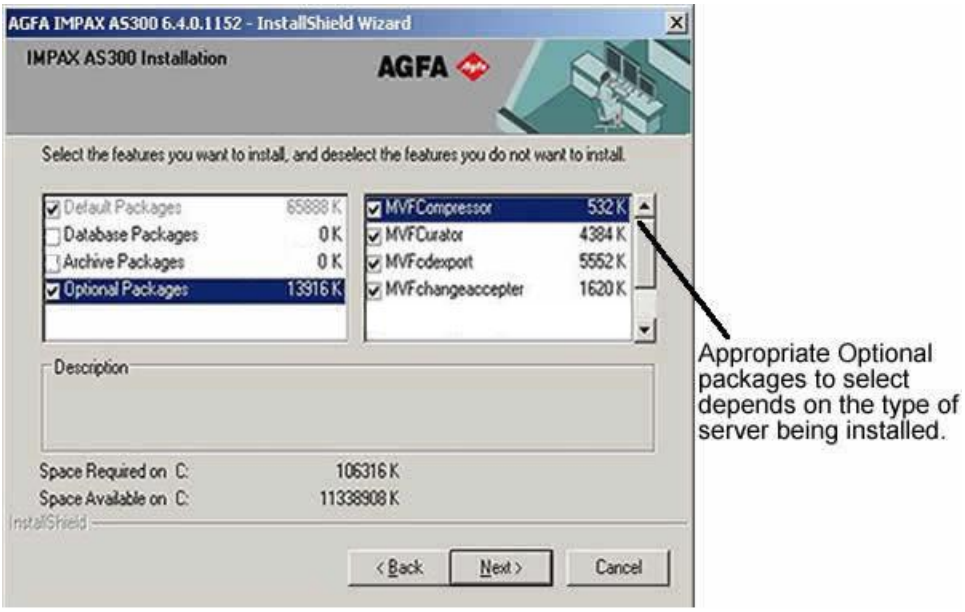
You can now install the AS300 software with the appropriate packages. If installing multiple Curators, install and configure the master Curator before installing the secondary ones.

To install the Curator and CD Export server software

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

   This information is recorded in the installer log file.
4. On the Welcome screen, click **Next**.
5. Clear the **Database Packages** checkbox.
6. Clear the **Archive Packages** checkbox.
7. Select the **Optional Packages** label and select the appropriate packages. **MVFCurator** must stay selected. **MVFcdexport** is also required except, perhaps, on slave Curators.

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



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

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

    The files are copied.
12. After all the packages have been installed, click **Yes, I want to restart my computer now**.

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

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

Migrating the master Curator from an all-in-one server to a separate server

(Topic number: 120824)

Use this procedure when migrating the Curator from an all-in-one server to a separate server.

Note:

After the migration, you can leave the former Curator as the slave Curator, or you can remove it. Instructions are provided in *Removing the Curator service from the slave Curator* (refer to page 92).

To migrate the master Curator from an all-in-one server to a separate server

1. Log into the master Curator machine—currently, the all-in-one server.

2. After all current Curator jobs have completed, in the Job Manager, halt the Curator job queue.
3. Install the Curator on a new machine by following the instructions in the *Curator and CD Export Server Installation Guide*.

   Note:

   Ensure that the ODBC connection points to the database server.

4. Log into the new Curator server and start IMPAX services.
5. To ensure that the new Curator's ae_ref is recorded in the database, open an SQL editor an run the following query:

   select * from map_ae where ae_title=*New _Curator_ae_title.*
6. In CLUI, display a list of services by typing the following:

   service query

   The service query command returns a list of services similar to the following:

```
ref       AE title      P. Title    Host      Port   Type       Protocol


1029      XMT65-SQL2K5  CURATOR     xmt65-sq  3056   SIGNAL     SIGNAL
1036      XMT65-SQL2K5  CURATOR     xmt65-sq  3055   PUBLIC     QUEUE
```

7. Using the results from the previous query, find the service_ref for the service with the appropriate values.
   - AE title = *new_Curator_AE_title*
   - P. Title = CURATOR
   - Type = PUBLIC

   In the example in step 6, the service_ref is 1036.
8. In CLUI, obtain the Curator queue_ref value by typing the following:

   queue query
9. Change the Master Curator service to the Curator installed on the new machine by running the following SQL Update statement:

   update map_queue set service_ref=*new_Curator_service_ref* where QUEUE_REF=*Curator_queue_ref*

   where *new_Curator_service_ref* is the service_ref value you obtained in step 7 and *Curator_queue_ref* is the value you obtained in step 8.
10. Change ownership of the web cache to the new master Curator by running the following updated statement:

    update osr_volume set ae_ref=*new_Curator ae_ref* where ae_ref=*old_curator ae_ref* and volume_type='W'

11. Change the ae_ref values for all studies located in the web cache by running the following update statement:

    update dosr_study_location set ae_ref =*new_curator_ae_ref* where ae_ref=*old_curator_ae_ref* and volume_type='W' and study_ref > *a_study_ref* and study_ref <= *another_study_ref*.

    Note:

    Do not update the more than 10,000 rows of the dosr_study_location table at a time.

12. Restart the Curator and Autopilot on the old and new Curator machines.
13. Restart the Curator queues.
14. Check in the master Curator log file to see if the following message appears:

    ```
    autopilot mvf_ap_controller_thread_class::initialize_autopilot(): Autopilot
    running on Master Curator, ae_ref <new_Curator_ae_ref>
    ```

    If you are leaving the former Curator as the slave, then check the slave Curator log file for the following message:

    ```
    autopilot mvf_ap_controller_thread_class::initialize_autopilot(): Autopilot
    running on Slave Curator with ae_ref <old_Curator_ae_ref>. Master Curator
    running in ae_ref <new_Curator_ae_ref>.
    ```

15. If you have decided to leave the former Master Curator as the slave Curator, test that both Curators are running by following these steps:
    a. On the slave Curator machine, stop the Mitra Task Scheduler process and the Curator.
    b. Send a test study and check that the study is curated.
    c. Restart the Mitra Task Scheduler process and the Curator.
    d. Restart the Curator queue on the master Curator.
    e. Ensure that both Curators and the Mitra Task Scheduler are running.
16. If you have decided that the new Curator (the Master Curator) will be the only Curator, test that it works by sending a test study. Check that the images were curated.
17. If you have decided to remove the former Curator (the slave Curator), remove the Curator service. b

    To do so, follow the instructions in *Removing the Curator service from the slave Curator* (refer to page 92).

Removing the Curator service from the slave Curator

(Topic number: 120864)

After migrating a Curator from an all-in-one server to a separate server, if you have decided to remove the former Curator (the current slave Curator), you must remove the Curator service from the slave machine.

To remove the Curator service from the slave Curator

1. Log into the server whose service you want to remove.
2. Ensure that all of the service's jobs have completed.
3. Using the Job Manager, halt all the queues.
4. Stop all IMPAX services.
5. On Windows 2003 server, open Control Panel and select **Add Remove Programs**.

   or

   On Windows 2008 server, open Control Panel and select **Programs and Features**.
6. Uninstall IMPAX.
7. To use this server with other IMPAX services, reinstall IMPAX and exclude the Curator service from the installation.
8. After the IMPAX installation is complete, restart the IMPAX services.
9. Open CLUI and remove the service_ref of the removed service by typing:

   service delete *service_ref*

   Note:

   Normally, every Process Title has two service_ref values—one of type SIGNAL, and one of type PUBLIC. You must delete both.
10. Restart all queues.

Upgrading the other IMPAX 6.5.1 components

9

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 complete the migration to IMPAX 6.5.1, the Application Server, Curator, and Clients must be upgraded, and a few configurations are required.

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

Parameters	Values	Default value
-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. Upgrading the Application Server from a previous version

(Topic number: 11188)

Important!

For AS300 Oracle and for all AS3000 (Solaris server) sites, before upgrading the Application Server, ensure that you have the correct version of Oracle 10g Client installed. For instructions on how to check the current version of the Oracle Client, see *Determining the version of the installed Oracle Client* (refer to page 100). For instructions on how to install the Oracle 10g Client, see *Installing and configuring the Oracle 10g Client for Windows* (refer to page 102).

Upgrade all Application Servers in the cluster to IMPAX 6.5.1.

Important!

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

Upgrading the ADAM database

(Topic number: 58664)

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

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

If you are upgrading a cluster to Windows Server 2008, you must replicate the ADAM database instance on a new Windows 2008 server, which uses the AD LDS database. For information on how to replicate the ADAM database on a Windows 2008 server, see *Migrating an Application Server from a Windows 2003 server to a Windows 2008 server* (refer to page 119).

Backing up the ADAM database

(Topic number: 6717)

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

To back up the ADAM database

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

The default location for the ADAM database is C:\Program Files\Microsoft ADAM\AgfaHealthcare.

10. If backing up to a tape drive, under Backup media type, select the tape drive, and in the backup media area, click **New media**. Click **Next**.

    or

    If backing up to any other media type, select the location where the backup is to be saved, and type a name for the backup. Click **Next**.
11. On the Completing the Backup Wizard screen, click **Advanced**.
12. On the Type of Backup screen, select **Normal.** Click **Next**.
13. On the How to Backup screen, select **Verify data after backup and Use hardware compression if available.** Click **Next**.
14. On the Backup Options screen, select **Replace the existing backups**. Click **Next**.
15. On the When to Backup screen, select **Now**. Click **Finish**.
16. In the Backup Progress dialog, click **Close**.
17. Close the Backup Utility.

Stopping services on the Application Servers

(Topic number: 10144)

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

To stop services on the Application Servers

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

Uninstalling IMPAX 6.2 documentation

(Topic number: 10736)

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

To uninstall the IMPAX 6.2 documentation

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

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

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

To uninstall IMPAX 6.3 or later documentation

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

4. Click **Remove**.
5. In the confirmation dialog, click **OK**.

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

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

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

To uninstall the IMPAX Installation Server

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

The Agfa IMPAX Installation Server is uninstalled.

Installing the recommended version of the Oracle Client

(Topic number: 106750)

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

Important!

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

Determining the version of the installed Oracle Client

(Topic number: 106578)

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

Important!

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

To determine the version of the installed Oracle Client

1. Open a command prompt.
2. Type

   sqlplus -V

If the command returns `SQL*Plus: Release 10.2.0.1.0 - Production`, version 10.2.0.1 is installed and needs to be uninstalled first. For further details, see *Removing ODBC entries prior to uninstalling the Oracle Client* (refer to page 101) and *Uninstalling the previous version of Oracle Client* (refer to page 101)

If the command returns `SQL*Plus: Release 10.2.0.4.0 - Production`, version 10.2.0.4 is installed and needs to be upgraded. For further details, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 105).

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

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

To remove ODBC entries prior to uninstalling the Oracle Client

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

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

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

CAUTION!

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

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

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

6. Click **Save**.

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

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

To uninstall the previous version of Oracle Client

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

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

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

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

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

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

Determine which Oracle Client is installed on the system; see *Determining the version of the installed Oracle Client* (refer to page 100). If Oracle Client version 10.2.0.1 is installed, uninstall it. If Oracle Client version 10.2.0.4 is installed, see *Upgrading to the 10.2.0.4 version of the Oracle Client for Windows* (refer to page 105).

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

Important!

Before installing the Oracle Client, disable virus protection software.

To install and configure the Oracle 10g Client for Windows

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

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

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

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

Note:

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

Setting up a connection to the Oracle database

(Topic number: 46341)

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

To set up a connection to the Oracle database

1. If the Net Configuration Assistant is not open, select **Start** > **All Programs** > **Oracle - ohome** > **Configuration and Migration Tools** > **Net Configuration Assistant**.
2. In the Oracle Net Configuration Assistant Welcome dialog, select **Local Net Service Name configuration** and click **Next**.

3. If the Naming Methods Configuration dialog appears, select **Local Naming**. Click **Next**.
4. In the Net Service Name Configuration screen, select **Add**. Click **Next**.
5. In the Service Name field, type **MVF**. Click **Next**.
6. From the list of protocols, select **TCP**. Click **Next**.
7. In the TCP/IP dialog, type the hostname of the Oracle server.
8. Accept the default port number (1521). Click **Next**.
9. Select **Yes, perform a test**. Click **Next**.

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

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

    or

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

Reconfiguring ODBC data source names
(Topic number: 67665)

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

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

To reconfigure ODBC data source names

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

where *Oracle_instance_name* is the name typed when *Installing and configuring the Oracle 10g Client for Windows* (refer to page 102).

6. Click **Finish**.
7. In the Data Source Name field, type **mvf**.
8. Type a description, if needed.
9. In the TNS Service Name field, type **MVF.world**.
10. In the User Name field, type **mvf**.

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

Upgrading to the 10.2.0.4 version of the Oracle Client for Windows

(Topic number: 106600)

Important!

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

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

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

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

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

The Oracle Client is upgraded.

Upgrading the IMPAX Application Server software to 6.5.1

(Topic number: 9863)

Important!

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

After backing up the ADAM database (refer to page 97), you can upgrade the Application Server software.

Note:

This installation does not overwrite the existing ADAM database.

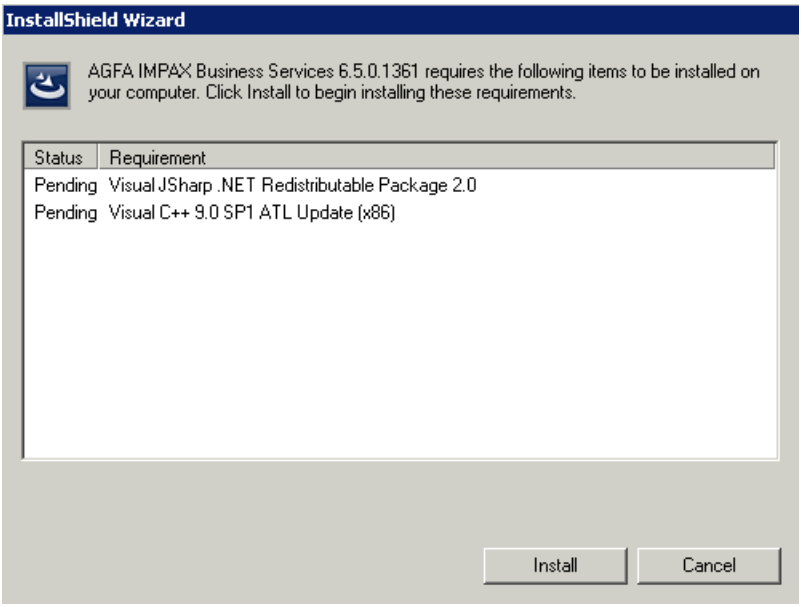
To upgrade the IMPAX Application Server software to 6.5.1

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

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

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

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



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

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

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 99). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 113).

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

To install the IMPAX documentation

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

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

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

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

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 117)) or on a separate, dedicated Windows-based server.

Note:

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

Therefore, we recommend:

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

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

The Installation Server Setup package contains:

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

- Links to the individual perquisites

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

CAUTION!

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

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

To run the IMPAX Installation Server package

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

   A Preparing to install message appears.

2. On the Welcome to the InstallShield Wizard for IMPAX Installation Server screen, click **Next**.

3. To install the application into C:\Inetpub\wwwroot\ClientInstaller, on the Destination Folder screen, click **Next**.

   or

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

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

   The first installer runs.

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

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

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

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

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

Running Healthcheck from a URL to check the status of web services
(Topic number: 11405)

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

Note:

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

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

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

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

   or

   If Healthcheck has been configured to automatically log in, type

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

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

CAUTION!

Setting the refresh interval below five seconds impacts performance.

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

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

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

Upgrading additional Application Servers in the cluster

(Topic number: 11210)

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

To upgrade additional Application Servers in the cluster.

1. Upgrade the IMPAX Application Server software (refer to page 106).
2. Verify the installation.

Upgrading the AD LDS database from IMPAX 6.5 to IMPAX 6.5.1

(Topic number: 130063)

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

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

Creating a one-time backup of AD LDS

(Topic number: 113662)

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

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

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

To create a one-time backup of AD LDS

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

   dsdbutil
3. At the dsdbutil prompt, type

   activate instance AgfaHealthcare
4. At the dsdbutil prompt, type

   ifm
5. At the ifm prompt, type

   create full *location*

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

   Example:

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

   quit

At the dsdbutil prompt, type

quit

The AD LDS instance is backed up.

Stopping services on the Application Servers

(Topic number: 10144)

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

To stop services on the Application Servers

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

Uninstalling IMPAX 6.3 or later documentation

(Topic number: 15533)

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

To uninstall IMPAX 6.3 or later documentation

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

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

All installed IMPAX documentation for the version selected is uninstalled.

Uninstalling the IMPAX Installation Server

(Topic number: 119239)

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

To uninstall the IMPAX Installation Server

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

The Agfa IMPAX Installation Server is uninstalled.

Upgrading the IMPAX Application Server software to 6.5.1

(Topic number: 126080)

Important!

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

After backing up the ADAM database (refer to page 97), you can upgrade the Application Server software.

Note:

This installation does not overwrite the existing ADAM database.

To upgrade the IMPAX Application Server software to 6.5.1

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

   For example, set the path to J:\wwwroot rather than C:\inetpub\wwwroot.

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

The Application Server software is upgraded.

Installing the IMPAX documentation

(Topic number: 15523)

The IMPAX 6.5.1 documentation is installed on the Application Server.

Before installing the IMPAX 6.5.1 documentation, ensure that you have uninstalled any earlier IMPAX documentation. Instructions on how to uninstall the IMPAX 6.2 or earlier documentation are in the topic *Uninstalling IMPAX 6.2 documentation* (refer to page 99). For IMPAX 6.3 and later, instructions are in *Uninstalling IMPAX 6.3 or later documentation* (refer to page 113).

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

To install the IMPAX documentation

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

   A `Preparing to install` message appears.
3. On the Welcome screen, click **Next**.
4. On the Setup Type screen, select the appropriate option and click **Next**.
   - To install all documentation in all available languages (up to 24 languages), select **All Documentation**.
   - To install all English-language documentation, select **All English Documentation**. This is the default.
   - To select which documentation to install in which languages, select **Select Documentation to Install**.

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

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

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

Installing the IMPAX Installation Server

(Topic number: 7773)

You may choose to install the Installation Server program on an IMPAX Application Server (in which case you can continue with *Running the IMPAX Installation Server package* (refer to page 117)) or on a separate, dedicated Windows-based server.

Note:

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

Therefore, we recommend:

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

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

The Installation Server Setup package contains:

- The installers (or links) for the IMPAX Client prerequisites:

- .NET Framework 3.5 SP1
- Visual C++ 9.0 SP1
- DirectX

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

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

CAUTION!

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

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

To run the IMPAX Installation Server package

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

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

   or

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

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

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

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

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

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

(Topic number: 11405)

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

Note:

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

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

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

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

   or

   If Healthcheck has been configured to automatically log in, type

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

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

CAUTION!

Setting the refresh interval below five seconds impacts performance.

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

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

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

Upgrading additional Application Servers in the cluster

(Topic number: 11210)

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

To upgrade additional Application Servers in the cluster.

1. Upgrade the IMPAX Application Server software (refer to page 106).
2. Verify the installation.

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

(Topic number: 109634)

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

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

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

3. 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*.

4. Upgrading Clients to IMPAX 6.5.1

(Topic number: 10176)

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

Important!

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

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

(Topic number: 7752)

Important!

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

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

To manually uninstall the IMPAX 6.2 or later Client software

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

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

Installing the IMPAX Client

(Topic number: 7776)

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

Note:

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

To install the IMPAX Client

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

   For information on setting up a Client installation server, refer to "*Installing the IMPAX Installation Server* (refer to page 116)" (topic number 7773) in the *IMPAX 6.5.1 Client Installation, Upgrade, and Configuration Guide* or the *IMPAX 6.5.1 Preparing to Upgrade Guide—IMPAX 4.5, 5.2, 5.3, or WEB1000 to IMPAX 6.5.1*.
2. If a File Download dialog appears, click **Open** or **Run**.

   A `Preparing to Install` message appears.

   If on Windows Vista, a cscript.exe prompt may appear. To run it, click **OK**.
3. If a prompt appears about downloading and installing missing components, click **OK**.
4. Follow the prompts to download and install Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5 SP1, or all.

Note:

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

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

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

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

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

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

   or

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

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

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

    The program is installed.

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

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

Post-upgrade checking and stabilization

10

Some tasks are performed after the 6.5.1 upgrade is complete.

1. 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.

2. Testing the installed software

(Topic number: 61185)

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

To test the installed software

1. On the IMPAX Database Server, run the Administration Tools and ensure that you can log in using the administration password.
2. On the Application Server, open a web browser and connect to http://localhost. Ensure that the "Welcome to IMPAX" page is displayed.
3. Run the IMPAX Client and ensure that you can log in using the administration password.

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. Synchronizing clocks on Windows-based IMPAX systems

(Topic number: 6752)

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

Note:

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

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

Synchronizing Windows servers to an external time source

(Topic number: 58717)

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

CAUTION!

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

To synchronize Windows servers to an external time source

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

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

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

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

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

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

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

Synchronizing Windows servers to an internal time source

(Topic number: 58720)

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

CAUTION!

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

To synchronize Windows servers to an internal time source

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

   It may take some time for this to take effect.

Note:

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

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

(Topic number: 58572)

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

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

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

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

(Topic number: 58569)

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

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

1. Open a command prompt.
2. Type

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

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

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

   w32tm /resync

8. 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.

9. 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**.

10. 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**.

11. Uninstalling the Cross-Cluster Dictation Interlock tool

(Topic number: 60396)

If you no longer have to synchronize the dictation status of studies between the previous version and the 6.5.1 IMPAX systems, you can uninstall the components of the Cross-Cluster Dictation Interlock tool.

To uninstall the Cross-Cluster Dictation Interlock tool

1. On the previous version IMPAX Application Server where the Cross-Cluster Dictation Interlock components were installed, open the Windows Administrative Tools and select **Services**.
2. Right-click the **Impax Study Status Relay** service and select **Stop**.
3. Close the Services window by selecting **File** > **Exit**.
4. Open a command prompt.
5. Change to the directory containing the Cross-Cluster Dictation Interlock components—possibly C:\Program Files\Agfa\Impax Business Services.
6. Type **uninstall_study_status_relay_service.bat**.
7. Close the command prompt by typing **exit**.
8. From Windows Explorer, navigate to and delete the **study-status-signal-relay** folder (possibly from C:\Program Files\Agfa\Impax Business Services).
9. On the IMPAX 6.5.1 Application Server where the 6.5.1 Cross-Cluster Dictation Interlock components were copied, follow steps 1 to 7.
10. Log into a previous version IMPAX Client as an administrator user.
11. From the Configure area - Users and Roles section, delete the **remote-dictation** user from the Study Status Relay role, then delete the **Study Status Relay** role.
12. Log into an IMPAX 6.5.1 Client as an administrator user and repeat the previous step on it.

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

Oracle Data Guard: Disaster recovery solution

A

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

What is Oracle Data Guard?

(Topic number: 65374)

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

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

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

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

   We recommend three times the database size for backup allocation.

3. A set of tools to monitor the configuration (refer to page 157).

To use Oracle Data Guard, the IMPAXoradg package (AS3000) or MVForadg package (AS300) must be installed; see *Installing the Oracle Data Guard package on a Database Server* (refer to page 135).

Configuring Oracle Data Guard

(Topic number: 65856)

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

Oracle Data Guard configuration overview

(Topic number: 66674)

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

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

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

   This will be the primary database.

2. On AS3000 machines, install the IMPAXoradg package as described in *Installing the Oracle Data Guard package on a Database Server* (refer to page 135). 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 135)

     or

   - Cold backup and restore (refer to page 139)

   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 145) 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 139). 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 136).
3. For Solaris servers only: Share the Flashback area.

4. Run the Oracle Data Guard configuration on the standby server (refer to page 137).
5. Complete the Data Guard configuration on the primary server (refer to page 138).
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 137).

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 138).

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 145) 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 135) 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 139).
2. Start the public listener (refer to page 140).
3. Run the Oracle Data Guard configuration on the standby server (refer to page 140).
4. For Solaris servers only: Share the primary Flashback and database areas (refer to page 141).
5. Restore the database on the standby server (refer to page 142).
6. Complete the Data Guard configuration by linking the two servers (refer to page 144).

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 140).

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 141); otherwise, if using Windows servers, restore the database on the standby server (refer to page 142).

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 142).

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.

Source directory	Source files	Target directory	Additionally
/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 144).

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 145) on the primary and standby servers.

Configuring RMAN backups after the Oracle Data Guard configuration

(Topic number: 66586)

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

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

To configure RMAN backups after the Oracle Data Guard configuration

1. Log into the primary server.

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

   sqlplus / as sysdba

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

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

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

   On Windows, use standard copy and paste functionality to copy the file over.
6. Log into the standby server as the **oracle** (Solaris) or **AgfaService** (Windows) user.

7. Run the **configure_backup** command on this server as well.
8. To shut down the standby server, type the following:

   sqlplus / as sysdba

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

    sqlplus / as sysdba

    startup mount

Maintaining Oracle Data Guard

(Topic number: 67248)

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

Synchronizing redo changes from the primary database to the standby database

(Topic number: 67142)

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

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

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

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

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

   alter database recover managed standby database cancel;

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

   alter system set standby_file_management = manual;

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

   connect internal

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

   select * from v$log;

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

   select * from v$logfile;

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

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

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

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

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

   alter system switch logfile;

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

   alter database drop logfile group #;

   select * from v$log;

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

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

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

    alter system set standby_file_management = auto;

Rebooting the standby database server

(Topic number: 67099)

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

To reboot the standby database server

1. Log into the standby server.

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

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

   $ sqlplus / as sysbda

   alter database recover managed standby database cancel;

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

   $ sqlplus / as sysbda

   startup mount;

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

   exit;
10. To start the private listener, type

    lsnrctl start listener

Rebooting the primary database server

(Topic number: 67102)

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

To reboot the primary database server

1. Reboot the primary server.

   On Solaris, log in as the **root** user and type **init 6**. On Windows, reboot the server.
2. After the reboot, verify that the public listener is started.

   On Solaris type **psg tns**. On Windows check that the **OracleohomeTNSListener_listener_public** service is started.
3. Start the public listener if not already started.

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

Resizing Oracle data files

(Topic number: 67133)

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

To resize Oracle data files

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

   alter system switch log file;

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

(Topic number: 67105)

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

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

1. Log into the primary server.

   On Solaris, log in as the **oracle** user. On Windows, log in as the **AgfaService** user.
2. In a command prompt, to run Data Guard manager, type

   dgmgrl sys/stayout@MVF1
3. In Data Guard manager, to remove the Data Guard configuration, type

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

   On Solaris, type

   cd /opt/oracle/current/dbs

   rm dr*.dat

   On Windows, delete the **dr*.dat** file from C:\oracle\product\10.2.0\db_1\database.
5. Save all the edited Data Guard files such as initMVF.ora, spfileMVF.ora, tnsnames.ora, and listener.ora. To make a copy of these files, type

   On Solaris:

   cd /opt/oracle/current/dbs

   cp initMVF.ora initMVF.ora.dg_save

cp spfileMVF.ora spfileMVF.ora.dg_save

cd /var/opt/oracle

cp tnsnames.ora tnsnames.ora.dg_save

cp listener.ora listener.ora.dg_save

On Windows:

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

cp initMVF.ora initMVF.ora.dg_save

cp spfileMVF.ora spfileMVF.ora.dg_save

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

cp tnsnames.ora tnsnames.ora.dg_save

cp listener.ora listener.ora.dg_save

6. To turn off flashback, type

   sqlplus / as sysdba

   alter database flashback off;

7. To turn off force logging, type

   alter database no force logging;

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

    sqlplus / as sysdba

    shutdown immediate;

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

    On Solaris:

    cd /opt/oracle/current/dbs

    cp –rp initMVF.ora.pre_dg initMVF.ora

    cd /var/opt/oracle

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

    On Windows:

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

    cp –rp initMVF.ora.pre_dg initMVF.ora

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

    cp –rp tnsnames.ora.pre_dg tnsnames.ora

    cp –rp listener.ora.pre_dg listener.ora

12. To create the spfile from the pfile, type

    sqlplus / as sysdba

    create spfile from pfile;

13. To start the database, type

    startup;

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

    On Solaris:

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

    On Windows:

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

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

Switching over to the standby server

(Topic number: 67114)

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

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

To switch over to the standby server

1. Stop the public listener on the primary server.

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

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

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

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

   dgmgrl sys/stayout@mvf1

   show configuration

switchover to 'MVF2'

show configuration

exit

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

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

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

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

   ae query

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

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

   Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete *service_ref*

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

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

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

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

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

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

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

Note:

If this is the first time that the standby database is opened after a switchover, re-create the temporary file on the standby server (refer to page 154).

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

Failing over to the standby server

(Topic number: 67117)

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

To fail over to the standby server

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

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

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

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

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

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

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

   dgmgrl sys/stayout@mvf2

   show configuration

   failover to 'MVF2'

   show configuration

   MVF2 is now the primary server.

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

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

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

   ae query

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

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

   Two service refs are returned.

7. For each service ref, in CLUI, type

   service delete <*service ref*>

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

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

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

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

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

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

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

Note:

If this is the first time that the standby database is opened after a failover, you must re-create the temporary file on the standby server (refer to page 154).

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

Re-creating the temporary file on the standby server

(Topic number: 67286)

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

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

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

   sqlplus sys/stayout as sysdba

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

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

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

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

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

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

4. To recreate TEMP01.DBF, type

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

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

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

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

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

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

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

   sqlplus sys/stayout as sysdba

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

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

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

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

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

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

4. To recreate TEMP01.DBF, type

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

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

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

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

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

Reinstating the failed primary database

(Topic number: 67120)

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

To reinstate the failed primary database

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

   sqlplus / as sysdba

   startup mount;

   quit

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

   dgmgrl sys/stayout@mvf2

3. To perform the switchover type

   show configuration

reinstate database 'MVF1'

show configuration

exit

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

   dgmgrl sys/stayout@mvf2

5. To make MVF1 the primary server type

   switchover to 'MVF1'

   exit

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

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

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

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

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

   ae query

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

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

   Two service refs are returned.

10. For each service ref, in CLUI, type

    service delete <*service ref*>

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

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

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

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

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

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

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

Tools for monitoring Oracle Data Guard

(Topic number: 66589)

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

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

Tip:

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

Troubleshooting: The application encountered a problem with the standby database

(Topic number: 66656)

Issue

The following error message appears in the Exception Viewer:

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

Details

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

Solution

Perform diagnostics such as the following.

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

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

   tnsping MVF

   tnsping MVF1

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

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

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

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

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

   select sequence#,applied from v$archived_log order by sequence#;
9. To force a log switch on the primary server, execute the command

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

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

    Ensure that one additional entry appears in the list.
11. To check the configuration, on the primary server, open the Data Guard manager:

    dgmgrl sys/stayout@mvf1

    show configuration;

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: 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: Application Server installation error

(Topic number: 96652)

Issue

When upgrading the Application Server, the following error appears:

```
Product: AGFA IMPAX Business Services -- Error 1335.The cabinet file 'Data1.cab'
required for this installation is corrupt and cannot be used. This could indicate
a network error, an error reading from the CD-ROM, or a problem with this package.
```

Details

Data1.cab files are left over from previous installations of the Application Server and cause problems with the InstallShield.

Solution

Delete all the Data1.cab files in the temp folder (%TEMP%).

Troubleshooting: Must back out of the Application Server upgrade

(Topic number: 60757)

Issue

A problem has occurred and I must return to the previous version of the Application Server software.

Solution

To back out of the Application Server upgrade

1. Back up the web.config files and note the location of the current web.config files.
2. On the Application Server, open Control Panel.
3. Select **Add or Remove Programs**.
4. Remove **AGFA IMPAX Business Services** and **IMPAX Installation Server**.

   Do not remove ADAM (Windows 2003) or AD LDS (Windows 2008).
5. Install the previous version (IMPAX 6.2 or later) of the Server, Application Server, and Client Installation Server software.

Note:

By installing an earlier version of the Client Installation Server, the Client workstation software is automatically rolled back within an hour for online workstations.

Troubleshooting: How do I determine which users are ADAM administrators?

(Topic number: 60661)

Issue

How do I determine which users are ADAM administrators?

Solution

If the site uses other dedicated Application Servers, you can determine which users on the Application Servers are ADAM administrators:

1. On an Application Server, select **Start** > **All Programs** > **ADAM** > **ADAM ADSI Edit**.
2. Select **Well-known naming context** and select **Configuration** from the list.

3. Click **OK**.

   If this step fails, you are not logged into the Application Server as an ADAM administrator. Log in as the user who originally installed ADAM or who has been added as an ADAM administrator and try these steps again.
4. Expand the new Configuration node and select **CN=Configuration** > **CN=Roles**.
5. Double-click **CN=Administrators**.
6. Double-click the **member** attribute.

   The ADAM administrators are listed by login name.

Troubleshooting: How do I determine which ADAM instance is the Schema Master?

(Topic number: 60664)

Issue

How do I determine which ADAM instance is the Schema Master?

Solution

If the site uses other dedicated Application Servers, you can determine which one is running the master ADAM instance to find out which is the Schema Master:

1. Select **Start** > **Run** and type **mmc**.
2. In the Console dialog, select **File** > **Add/Remove Snap-in**.
3. In the Add/Remove Snap-in dialog, click **Add**.
4. From the Snap-in list, select **ADAM Schema** and click **Add**.
5. To close the Add Standalone Snap-in dialog, click **Close**.
6. To close the Add/Remove Snap-in dialog, click **OK**.
7. Right-click ADAM Schema and select **Change ADAM Server**.
8. In the Connect to ADAM Server dialog, enter localhost as the ADAM server and add the port, usually 389.
9. Select This Account and select a user that is an ADAM Administrator from the list.
10. Click **OK**.
11. Right-click ADAM Schema and select **Operations Master**.

    The current Schema Master is listed in the dialog. This is the Application Server on which to upgrade the ADAM database.

Troubleshooting: Reinstalling Oracle on Windows

(Topic number: 121676)

Issue

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

CAUTION!

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

Solution

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

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

   delete oradim -DELETE -SID MVF

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

   CAUTION!

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

6. Select **Start** > **Oracle - ohome** > **Oracle Installation Products** > **Universal Installer**.

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

Note:

The AS300 installation automatically creates the MVF DSN.

Troubleshooting: 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

Upgrade and installation tool reference

C

More information is provided here about the AS300 installers and the cache check tools.

IMPAX AS300 installation programs

(Topic number: 7684)

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

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

Note:

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

32-bit AS300 installer packages reference

(Topic number: 7682)

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

Default

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

Database

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

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

Archive

Archive packages	Purpose
MVFhsm	Installs the HSM package.

Archiving considerations:

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

Optional

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

Optional packages	Purpose
MVFCompressor	Installs the MVF Compressor package, which includes mvf_compressor_scheduler. The mvf_compressor_scheduler process is responsible for scheduling the lossy compression of images.
MVFCurator	Installs the Curator package. The Curator process compresses incoming images into Mitra wavelet format and stores them in the web cache. Studies compressed by the Curator process are served locally or over a network to display clients.
MVFcdexport	Installs the CD Export server, used with the CD Export feature in the IMPAX Client. The CD Export server processes local burn jobs created by the IMPAX Client and prepares the zip files containing the data for the burn job. For instructions on using CD Export, refer to "Exporting and viewing images from CD or DVD" (topic number 8209) in the *IMPAX 6.5.1 Client Knowledge Base: Extended*.

Optional packages	Purpose
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).

64-bit AS300 installer packages reference

(Topic number: 65290)

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

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

Optional packages	Purpose
MVForadg	Installs a set of scripts and tools for configuring and monitoring Oracle Data Guard. Data Guard is Oracle's high-availability solution. **Important!** Data Guard works **only** on servers running Oracle Enterprise Edition. Do not install it on a database server using SQL Server

Optional packages	Purpose
	or Oracle Standard Edition, and do not include it on other types of servers (Archive Server, Network Gateway, Curator).

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

IMPAX packages found in the registry

(Topic number: 58575)

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

Note:

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

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

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

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

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

Cache check tools reference

(Topic number: 60457)

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 174) mvf-clean-cache (refer to page 174), and mvf-ddo-rescue (refer to page 175), 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.

External software licenses

D

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

AutoFac 2.1.13

(Topic number: 121742)

Autofac IoC Container

Copyright (c) 2007-2008 Autofac Contributors

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

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

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

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

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

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

Cygwin

(Topic number: 121758)

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

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

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

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

Preamble

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

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

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

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

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

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

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

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

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

END OF TERMS AND CONDITIONS

Editline 1.2-cstr

(Topic number: 121768)

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.

Log4Net

(Topic number: 7648)

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

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

Administration Tools

Administration Tools control the configuration and management of the entire IMPAX cluster. The Administration Tools are a Java-based application that run in a web browser.

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.

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

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

master Curator

When using multiple Curators, the first Curator that runs, which owns the job queue.

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.

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.

W

wizard

Wizards are used to automate processes. Wizards perform a predetermined sequence of actions after they are selected and applied.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z