IMPAX 6.3

AS300 Configuration Guide

Configuring IMPAX in a Single-Host, Multi-Host, or Mixed-Host Configuration

AGFA

Agfa

see more | do more

Copyright information

Trademark credits

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-Gevaert N.V. makes 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-Gevaert 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-Gevaert 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.

2007-5-9

Revision record

Document name: IMPAX 6.3 AS300 Configuration Guide

Revision date	Description
May 2007	Released for publication

Manufacturer's responsibility

The manufacturer, installer, or importer will be responsible for 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.

Additional documentation

This guide is intended for service and administrative personnel who are installing or upgrading, configuring, and maintaining the server components of the IMPAX 6.3 system.

For information about using the IMPAX software once it is installed, refer to the *IMPAX 6.3 Server Knowledge Base*, *IMPAX 6.3 Application Server Knowledge Base*, and *IMPAX 6.3 Client Knowledge Base*. These Knowledge Bases are installed on the Application Server. Refer to *Installing the IMPAX documentation* in Chapter 3 of the *IMPAX 6.3 Application Server Installation and Upgrade Guide*.

To open the IMPAX 6.3 Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed, and that you know the name of the Application Server it is installed on.
2. In a browser, navigate to:

   https://<*app_server_name*>/impax/documents/server/default.htm

To open the IMPAX 6.3 Application Server Knowledge Base

1. Ensure that the IMPAX documentation has been installed.
2. On the Application Server, double-click the **IMPAX 6.3 Application Server Knowledge Base** desktop shortcut.

   or

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

To open the IMPAX 6.3 Client Knowledge Base

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

Contents

Summary of IMPAX AS300 Server configuration steps

1

The following provides an overview of all steps required to configure an IMPAX AS300 Server. Details are provided in subsequent chapters.

Configuring IMPAX on an AS300 single-host server

To configure the single-host server, perform the tasks listed in the table that follows. For more complete instructions, refer to *Configuring an AS300 single-host Server or dedicated Database Server* (refer to page 9)

☑	Action
	Perform the initial database backup (refer to page 9)
	If required, configure database backup times (refer to page 10)
	Configure SQL Server character support (refer to page 11)
	Set up image and web caches (refer to page 14)
	Configure PACS Store and Remember archiving (refer to page 22), if using this type of archiving
	Configure an HSM archive (refer to page 28), if using this type of archiving
	Move the DVD-R archive VOLUMES partition (refer to page 28), if applicable
	If you have installed the Scavenger package, install and start the Scavenger service (refer to page 9)
	Change the default log file location (refer to page 30)
	Change the Administration Tools log file locations (refer to page 17)
	Create IPSEC filters to allow access to specified hosts (refer to page 31)

☑	Action
	If required, change the default Curator INI settings (refer to page 19)

Configuring IMPAX on a dedicated AS300 Database Server

You must configure the Database Server in the order listed in the table that follows. For more complete instructions, refer to *Configuring an AS300 single-host Server or dedicated Database Server* (refer to page 9).

☑	Action
	Perform the initial database backup (refer to page 9)
	If required, configure database backup times (refer to page 10)
	Configure SQL Server character support (refer to page 11)
	Identify any remote PACS in IMPAX (refer to page 13)
	Set up the image and web caches (refer to page 14)
	Change the default log file location (refer to page 30)
	Change the Administration Tools log paths (refer to page 17)
	Create IPSEC filters to allow access to specified hosts (refer to page 31)

Configuring IMPAX on an AS300 Archive Server

You must configure the Archive Server in the order listed in the table that follows. For more complete instructions, refer to *Configuring the Archive Server or Network Gateway* (refer to page 22).

☑	Action
	Set up the image and web caches (refer to page 14)
	Configure PACS Store and Remember archiving (refer to page 22), if using this form of archiving
	Configure an HSM archive (refer to page 28), if applicable
	If you have installed the Scavenger component, install and start the Scavenger service (refer to page 29)
	If applicable, move the DVD-R VOLUMES partition (refer to page 28)
	Change the default log file location (refer to page 30)
	Create IPSEC filters to allow access to specified hosts (refer to page 31)
	Where required, change the default Curator INI settings (refer to page 19)

Configuring IMPAX on an AS300 Network Gateway

You must configure the Network Gateway in the order listed in the table that follows. For more complete instructions, refer to *Configuring the Archive Server or Network Gateway* (refer to page 22).

☑	Action
	Set up the image and web caches (refer to page 14)
	Change the default log file location (refer to page 30)
	Create IPSEC filters to allow access to specified hosts (refer to page 31)
	If required, change the default Curator INI settings (refer to page 19)

2 Configuring an AS300 single-host Server or dedicated Database Server

After you have installed the necessary IMPAX packages on an AS300 single-host or AS300 Database Server and have installed the Application Server, configure the system components for initial use. If the database is an Oracle Database Server on a Solaris host (in a mixed-host configuration), refer to the *IMPAX 6.3 AS3000 Installation and Configuration Guide* instead. For more information on how to configure the IMPAX system using the Administration Tools, refer to the Administration Tools component of the *IMPAX 6.3 Server Knowledge Base*.

Performing the initial database backup

To guard against information loss, you must back up the information to 4mm tapes or disk on a daily basis. In case of a system failure, the database can then be restored by Agfa HealthCare or your local vendor from the copy.

CAUTION!

If you are using a tape backup, to ensure that you have up-to-date backups and backups in reserve, change the tape daily. Otherwise, the daily backup overwrites the contents of the tape in the drive.

You must do an initial manual backup of your database. Otherwise, SQL Server assumes that you do not want transaction logs maintained.

CAUTION!

If backups are not created on a regular basis, the transaction log fills up and eventually halts the operation of your system.

To back up a database using the Enterprise Manager

1. 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** > <*database name*>

   where <*server*> is the name of the SQL Server that the program is running under and <*database name*> 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.

   Ensure that the **Verify upon completion** option is selected.
5. To start the backup, click **OK**.
6. Exit the SQL Server Enterprise Manager.

To back up the database from the command line

1. At a command prompt, 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 of the tape/disk device.

Configuring database backup times

A schedule_backup job is automatically installed and enabled with the SQL Server software package. This backup is scheduled to run at 12:00 AM every day. In addition to the schedule_backup job, you can enable and schedule the differential or incremental database backup jobs, if required.

To configure an additional time to run a database backup, follow this procedure.

To configure database backup times

1. Ensure that you have done an initial manual backup of your database.
2. Select **Start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**.
3. In the Explorer window of the Enterprise Manager, expand **Console Root** > **Microsoft SQL Servers** > **SQL Server Group** > <*server*> > **Management** > **SQL Server Agent**.

   where <*server*> is the name of the SQL Server the program is running under.
4. Double-click **Jobs**.

5. In the Jobs dialog, right-click **schedule_backup** and select **Properties**.
6. Switch to the **Schedules** tab.
7. Click **New Schedule**.
8. In the New Job Schedule dialog, in the **Name** field, type **Daily Backup**.
9. To change the default weekly recurrence, click **Change**.
10. In the Edit Recurring Job Schedule dialog, under Occurs, select **Daily**.
11. If required, change the default time under Daily Frequency using the **Occurs Once at** option.
12. To apply the change, click **OK**.
13. To close the New Job Schedule dialog, click **OK**.
14. If you are backing up to disk:
    a. Switch to the **Steps** tab.
    b. Double-click **Step 1**.
    c. To set up the disk backup, in the command field, type:
    exec sp_backup_database @dump_device_name='disk_backup1'
    d. To apply the change, click **OK**.
15. To close the Job Properties dialog, click **OK**.
16. Exit the SQL Server Enterprise Manager.

Configuring SQL Server character support

Configure the MVF SQL Server driver to prevent problems with displaying some character types. Change only the information noted.

To configure character support

1. On Windows 2003, select **Start** > **Administrative Tools** > **Data Sources (ODBC)**.
   On Windows XP (standalone stations only), open Control Panel and select **Administrative Tools** > **Data Sources (ODBC)**.
2. Switch to the **System DSN** tab.
3. Select the **MVF SQL Server** driver.
4. Click **Configure**.
5. Click **Next**.
6. In the **Login ID** field, type **mvf**.
7. In the **Password** field, type the password for the mvf account. Click **Next**.
8. Click **Next**.
9. Clear the **Perform translation for character data** checkbox.
10. Click **Finish**.
11. To test the configuration, click **Test Data Source**.
12. To exit the test dialog, click **OK**.

13. To exit the setup dialog, click **OK**.
14. Close the ODBC Data Source Administrator dialog.

Logging into the Administration Tools

Many IMPAX Server configuration tasks must be performed in the Administration Tools. This topic explains how to log into the Administration Tools. A valid user ID and password are required.

Note:

Passwords are case-sensitive; *PASSWORD* is not the same as *password*.

To launch the Administration Tools locally

1. Select **Start** > **All Programs** > **MVF Administration Tools** > **Administration Tools**.
2. From the **Domain** list, select the correct domain.
3. In the **User ID** field, type the user ID assigned to you.
4. In the **Password** field, type your password.
5. Press **Enter** or click **Login**.

To launch the Administration Tools remotely

1. Select **Start** > **All Programs** > **Internet Explorer**.

   or

   Double-click the **Internet Explorer** desktop shortcut.
2. In the **Address** field, type the URL or IP address of the server.

   The Administration Tools launch in a new browser window.
3. From the **Domain** list, select the correct domain.
4. In the **User ID** field, type the user ID assigned to you.
5. In the **Password** field, type your password.
6. Press **Enter** or click **Login**.

Tip:

After you log in under your user ID for the first time, your user ID may appear as a button on the login screen. This can be configured by your system administrator. If your user ID appears as a button, you can click your User ID and type your password to log in.

Identifying remote PACS in IMPAX

This topic applies only to a dedicated Database Server.

When installing a new IMPAX 6.3 cluster, the database is automatically updated with the details for all Archive Server, Network Gateway, Curator, and CD Export server components within the cluster. These do not have to be configured as stations in Network Management.

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

Note:

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

Follow these instructions for each external PACS that IMPAX 6.3 can communicate with.

To set up a station in the Administration Tools

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

   For details, refer to "Defining types of communication between stations and the Server" (article ID 9000) in the Administration Tools component of the *IMPAX 6.3 Server Knowledge Base*.
7. Clear the **Send/Receive LEI only** checkbox.

   Note:

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

Tip:

For more information on adding stations, refer to the Administration Tools component of the *IMPAX 6.3 Server Knowledge Base* .

Understanding IMPAX image and web caches

When images are sent into IMPAX from an acquisition station or retrieved from an archive, they must be stored temporarily in an accessible location. This temporary storage area is called a *cache*. A cache is a set of directories on local or external hard disks.

IMPAX supports two types of caches: image and web. The image cache contains what in the IMPAX Client is called *original images*—the images as they are sent from the acquisition station. The web cache contains copies of the original images that have been compressed with wavelet encoding by the Curator component. In many cases, the version of image in web cache is faster for Clients to load.

You use the Cache Manager in Administration Tools to create cache volumes on stations and to set the priority for cache usage. The archive must have at least one cache it can use. If using the Curator component, it requires at least one web cache.

Creating a cache volume

Use the Cache Manager to specify partitions or subdirectories on stations to use as image cache or web cache. You can create cache volumes only from the server where the Administration Tools are installed; you cannot do so remotely through a browser login.

To create a cache volume

1. On the Daily tab, click **Cache Manager**. 
2. Click **New Cache Volume**. 
3. In the Add Volume dialog, select the **Volume Type** to create: **Image Cache** or **Web Cache**.
4. From the **Station** list, select the station to set up the cache on.

   For a web cache, select the station that the master Curator runs on.
5. In the **Path** field, type the path for the new cache volume.

   You must specify the cache locations using UNC paths.
6. Click **Add**.
7. In the Warning dialog, verify that the path is correct and click **Yes**.
8. To select the cache volume to fill with images first, click **Increase Priority** or **Decrease Priority**.
9. If the cache volume is hosted remotely or if you are setting up network area storage (NAS), after the cache is created, create a user account for the ImpaxServerUser on the system hosting the cache and give the ImpaxServerUser full read, write, and execute permissions on the cache folder. For details, refer to "Configuring web cache folder permissions" in the *IMPAX 6.3 Curator and CD Export Server Installation Guide*.

Considerations when defining the cache volume path

- When creating a cache on a Windows system, do not use a trailing slash or backslash at the end of the volume path. For example, when creating an image cache, do not type \\server\f$\CACHE1\; instead, use \\server\f$\CACHE1. Defining the cache volume with a trailing slash or backslash can cause problems in retrieving images from the cache.
- If Curator and Network Gateway components are installed on the same server, all caches on the system (image and web) must be shared. Shared caches are specified without the volume letter; for example, instead of \\server\f$\CACHE1, use \\server\CACHE1.

Note:

If cache volumes are assigned to a subdirectory on a partitioned hard drive, the values shown in the Available and Occupied columns in Cache Manager refer to the entire partition, not the subdirectory.

Configuring archives on a single-host server

The archive component of the single-host server requires some configuration. Refer to the topic applicable to the type of archiving being used.

Archive type	Applicable topic
PACS Store and Remember	*Configuring PACS Store and Remember archiving* (refer to page 22)
HSM	*Configuring an HSM archive* (refer to page 28)
DVD-R	*Moving the VOLUMES partition for DVD archives* (refer to page 28)

If using the Scavenger service, also refer to *Configuring Scavenger* (refer to page 29).

Logging out of the Administration Tools

Log out of the Administration Tools when you leave the station for any length of time. Logging out protects patient confidentiality, and maintains system security.

To log out of the Administration Tools

1. In the top-right corner of the Administration Tools, click **Exit**.
2. To close the Administration Tools window, click **Exit**.

When you log out, IMPAX continues to function in the background.

Configuring the default log file location

When IMPAX was installed, the operational log files location is set to C:\mvf\data\logs. If you have created a separate log file partition as outlined in the *IMPAX 6.3 AS300 Installation Guide*, you may want to update the default logging location to write to that partition.

Note:

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

For an AS300 single-host server, the following is the list of IMPAX services that can be modified:

Service	Process
DICOM Service Class Provider	SCP
DICOM Service Class User	SCU
DICOM Storage Cache Manager	Autopilot
DICOM Storage Cache Server	SPFTPD
DICOM MVF Library Manager	Jukebox archive
DICOM MVF Standalone Storage	Non-jukebox archive
MVF HSM Archive	HSM archive
Mitra Compressor Scheduler	Lossy Compression Scheduler
Mitra System Archive Scavenger	Scavenger
Mitra System Compressor	Lossy Compressor
Mitra System Task Scheduler	Task Scheduler

For a dedicated AS300 Database Server, the following IMPAX services can be modified to write to the LOGS partition.

Service	Process
DICOM Service Class Provider	SCP
Mitra Compressor Scheduler	Lossy Compression Scheduler
Mitra System Task Scheduler	Task Scheduler

Note:

Not all services may exist on the server.

Updating the IMPAX Server log file locations

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

To update the IMPAX log file locations

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

      -f *<full path of log file>*

      For example, **-f g:\log\mitra.log**.
   d. To restart the service, under Service status, click **Start**.
   e. To exit the Properties dialog, click **OK**.

Note:

You must start the service before exiting the Properties dialog; otherwise, your changes are not saved.

Updating logging for the Administration Tools server

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

To update logging for the Administration Tools server

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

   logDirectory

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

   mtk.logFile

   jmtk.logFile

   

   Note:

   Use the forward slash (/) in the path names.
3. To resume services, restart the Administration Tools server.

Creating IPSEC filters to allow access to specified hosts

The IMPAX security policy blocks some TCP ports used to communicate with hosts outside the IMPAX cluster. If you are connecting to other hosts, such as a domain controller or proxy server, create IPSEC filters to allow IMPAX to access the host. The filter allows all traffic to and from the host on all ports.

Note:

If the Application Server is installed on the same machine as the IMPAX Server, the Application Server creates the necessary filters for the domain controller.

To create a domain controller policy filter

1. Open Control Panel.
2. Select **Administrative Tools**.
3. Select **Local Security Policy**.
4. Select **IP Security Policies on Local Computer**.
5. Double-click **Impax Server Policy**.
6. In the IMPAX Server Policy Properties dialog, click **Add**.
7. Follow the Security Rule Wizard and the IP Filters Wizard, accepting the defaults except where noted in the following table. The IP Filters Wizard is launched from within the Security Rules Wizard.

To assist you in determining what selections and entries to make in each dialog, we have included examples for creating a filter for a domain controller. Substitute the appropriate information for the host you are accessing.

Wizard	Screen	Options
Security Rule Wizard	Tunnel Endpoint	1. Accept default selection, **This rule does not specify a tunnel**.
Security Rule Wizard	Network Type	1. Change to **Local area network (LAN)**.
Security Rule Wizard	Authentication Method	1. Accept the default authentication method.
Security Rule Wizard	IP Filter List	1. Click **Add.**
Security Rule Wizard	IP Filter List	1. In the **Name** field, type an appropriate name for the filter. Example: Domain Controller Filter List 2. In the **Description** field, type an appropriate description for the filter.

Wizard	Screen	Options
		Example: Open access to the domain controller 3. Ensure that **Use Add Wizard** is enabled. 4. Click **Add**. The IP Filter Wizard is launched.
IP Filter Wizard	IP Filter Description and Mirrored property	1. Add an appropriate description. Example: **Open Access to the Domain Controller** 2. Enable **Mirrored**.
IP Filter Wizard	IP Traffic Source	1. From the **Source** address list, select **My IP Address.**
IP Filter Wizard	IP Traffic Destination	1. From the **Destination** address list, select one of**:** • **A specific DNS Name**—If the hostname is known. • **A specific IP Address**—If the IP address is known. 2. Type the fully qualified hostname or IP address. 3. If you typed a hostname and received a security warning about creating a filter using the hostname, review the content of the message for correctness and then, to create the filter, click **Yes**.
IP Filter Wizard	IP Protocol Type	1. From the **Select a protocol type** list, accept the default selection for **Any**.
IP Filter Wizard	Completing	1. Click **Finish**.
Security Rule Wizard	IP Filter List	1. Click **OK**.
Security Rule Wizard	IP Filter List	1. Select the filter you just created. Example: Domain Controller Filter List 2. Click **Next**.
Security Rule Wizard	Filter Action	1. Select **Impax Permit Action**.

Configuring Curator INI settings

If you are installing Curator on a separate machine, or on multiple machines in a master-slave configuration, you should do this after configuring all the IMPAX Server components. For installation details, refer to the *IMPAX 6.3 Curator and CD Export Server Installation Guide*.

If you have installed Curator on a single-host, Archive, or Network Gateway server, configure the Curator settings. The Curator settings control how all Curators process images for the web cache. Although the Curator settings do not exist in the map_ini table when the system is first installed, the default behavior applies. To change the default behavior to suit your site, add the appropriate settings and values.

To configure Curator INI settings

1. In CLUI, to add a new Curator setting, type:

   INSERT INTO map_ini (ini_section, ini_key, ini_value) VALUES ('CURATOR', '<*ini_key*>'<*ini_value*>**')**

   or

   To update an existing Curator setting, type:

   UPDATE map_ini SET ini_value=<*ini_value*> **WHERE ini_section="CURATOR" AND ini_key=**"<*ini_key*>"

   where <*ini_key*> is the Curator setting to change and <*ini_value*> is the updated value.

2. To prompt any Curator processes that are running to refresh their configuration settings for subsequent jobs, type:

   SIGNAL database_updated

Curator INI settings: Reference

The following table explains the Curator INI keys and their possible values.

ini_key	Default value	Description of possible values
AUTO_DELETE	F	T—Delete the study from the image cache when the web representation is created. Curator does not delete images or other non-image objects from the image cache that it has not created web representations for. The web cache copy cannot be sent to other PACS systems. F—Keep the image cache version as well as the web cache version. The image cache copy can be sent to other PACS systems. **Note:** Images compressed using Mitra Wavelet compression take longer to decompress than images compressed using standard compression. To provide faster access to images for local clients, configure Curator to keep image cache copy. We do not recommend deleting the image cache copy unless the server is configured to function strictly as a web server.

ini_key	Default value	Description of possible values
COLLECT_PERFORMANCE_METRICS	T	T—Collect performance metrics on prepare jobs and store them in map_job_metrics table. F—Do not collect performance metrics. The following metrics are recorded in the map_job_metrics table: • SERVICE_REF—Service ref of the curator process that handled the prepare job. • NUM_OBJECTS—Number of objects in the study being curated. • STAT1—Number of frames that were curated. • STAT2—Input size of study in MB. • STAT3—Raw size of study in MB. • STAT4—Amount of data written to web cache in MB.
DELETE_DUPLICATE_JOBS	T	T—Duplicate PREPARE jobs are deleted. F—Duplicate PREPARE jobs are allowed.
MIN_MEM_FREE	300	Minimum amount of free memory, in MB, that Curator requires. If the amount of free memory falls below this number, Curator restarts. To have Curator ignore this, set the MIN_MEM_FREE to -1. If you change this from the default, select a value that is at least 6 times the uncompressed size of the largest image you intend to curate.
QFACTOR_REUSE	F	T—The Q Factor is reused between compatible images/frames within the series. F—The Wavelet Q Factor defined in the Web Compression Manager is ignored and the Q Factor is not reused. We do not recommend changing this setting to T (True).
SEND_SIGNALS	T	T—Send STUDY-SIMPLIFIED MAP signal to the Client. F—Do not send the signal to the Client.

Configuring the Archive Server or Network Gateway

3

After you have installed the necessary IMPAX packages on the Archive Server or Network Gateway, the system components can be configured for initial use. Configuration must be performed after the IMPAX Server software and the Application Server software is installed. For procedures and information on how to configure the IMPAX system using the Administration Tools, refer to the Administration Tools component of the *IMPAX 6.3 Server Knowledge Base*.

Configuring PACS Store and Remember archiving

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).

PACS Store and Remember archiving is used in two circumstances:

- When an external PACS system is used as the primary archive device (there is no archive hardware on the IMPAX system)
- As additional storage in a cluster with separate archive servers connected to other archive types, for example, separate hub and spoke IMPAX clusters (two or more) or an external PACS with current or historical image data

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

The difference between PACS Store and Remember archiving and media-based archiving is that the MVF_SCU process handles the archiving instead of a separate archive process. With PACS Store and Remember archives, STORE jobs are done via DICOM C-STORE and RETRIEVE jobs are done via DICOM C-MOVE. In media-based archiving, the STORE and RETRIEVE jobs are handled by internal processes.

PACS Store and Remember Archiving is also known as PACS Archiving.

To set up PACS Store and Remember archiving

1. Obtain and install (refer to page 23) an archive license key on the PACS Store and Remember archive server.
2. Add the PACS Store and Remember archive in Network Management (refer to page 23).
3. Register the PACS Store and Remember archive services (refer to page 24).
4. Test the PACS Store and Remember archive functionality (refer to page 24).

Installing the archive license key

Ensure that you have obtained the archive license key for the server from Agfa.

Using PACS Store and Remember archiving (or any other type of archiving) requires an archive license key. If you have not already installed on the server, do so now.

To install the archive license key

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

   The license key name is the MAC address with a .lic file extension.
2. Select **Start** > **All Programs** > **Accessories** > **Windows Explorer**.
3. Copy the archive license key to the C:\mvf directory on the hard drive.
4. Rename the license key to **mvfarch.lic**.

Setting up the PACS Store and Remember archive in the Administration Tools

To configure an external PACS archive as a PACS Store and Remember archive, set up the external PACS archive in Network Management in the IMPAX Administration Tools.

Note:

If you are using different AE titles on the external PACS archive for store jobs and retrieve jobs, steps 3 to 11 must be followed twice: once for the store AE title, and once for the retrieve AE title.

To add a Store and Remember archive in Network Management

1. Launch and log into the Administration Tools.
2. On the Setup tab, click **Network Management**. 
3. To set up a new destination, click **New**. 
4. In the **AE Title** field, type the AE title of the external PACS archive.
5. In the **Alias** field, type an alias for the archive.

6. In the **Host** field, type the hostname or IP address.
7. Click **Save**.
8. Switch to the **Capabilities** tab.
9. From the list at the bottom of the manager, select the external PACS archive.
10. Under Station Type, select **PACS**.
11. Under Server is Allowed to, select **Query/Retrieve from Station**.
12. Click **Save**.
14. Register the PACS Store and Remember archive services in Windows (refer to page 24).

Registering PACS Store and Remember archive services in Windows

Designate the server that will perform the PACS Store and Remember archiving. Often this is the server running the Network Gateway software.

To register PACS Store and Remember archive services in Windows

1. Open Control Panel.
2. Select **Services**.
3. Make sure the **Service Class User** service is started.
4. Close the Services and Control Panel windows.
5. At a command prompt, type:

   cd \mvf\bin

   install_pacs.bat *<AE title of the PACS Store and Remember archive> <AE Title of the external PACS archive> <AE Title for retrieve jobs on the external PACS archive>*
6. Open Control Panel.
7. Select **Services**.
8. Right-click the **Service Class User** service and, if running, select **Stop**.
9. Right-click the **Service Class User** service and select **Start**.
10. Close the Services and Control Panel windows.

Testing PACS Store and Remember archiving

Test the PACS Store and Remember archive to make sure the services were registered properly.

To test that the archive was set up correctly

1. To confirm that the external archive is set up correctly in IMPAX, check that the external archive is listed in the /etc/hosts file.
2. To confirm that the external archive can be accessed, ping the external archive using the hostname or IP address.

To test store and retrieve functionality

1. Launch and log into the Administration Tools.
2. On the Daily tab, click **Job Manager**. 
3. Ensure that a PACS Archive queue exists.
4. On the Daily tab, lick **Study Manager**. 
5. Search for and select a study to store to the PACS Store and Remember archive.
6. To test the store functionality, click **Store to Archive**. 
7. If you are using more than one archive, from the **Archive** list, select the PACS Store and Remember archive and click **OK**.
8. Ensure that the study is stored to the PACS Store and Remember archive.
9. To delete the study from the local cache so you can test the retrieve functionality, from the **Location** list, select **Cached**.
10. Search for and select the study you stored to the PACS Store and Remember archive.
11. Click **Delete from Cache**. 
12. Confirm that you want to delete the selected study from cache.
13. To test the retrieve functionality, from the **Location** list, select **Archived**.
14. Search for and select the study in the PACS Store and Remember archive.

    If they study is stored in more than one location, ensure that you select the copy in the PACS Store and Remember archive.
15. Click **Retrieve**. 

Configuring a PACS Archive Provider (PAP)

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 at one PACS to be viewed at another. This can be achieved effectively using the PACS Archive Provider (PAP).

A PACS Archive Provider (PAP) acts like a Service Class Provider (SCP) by receiving 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. Also, the PAP can parse the private tags of the incoming DICOM objects to determine the objects' HIS verification and study status. This eliminates the need to HIS verify a study a second time or to add the incoming study to a radiologist's worklist.

To configure automatic archiving of studies by the PAP

1. Configure a source to send to the PAP component, which listens on port 9104.
2. On the PACS that contains the PAP, configure PACS Store and Remember archiving. Refer to *Configuring PACS Store and Remember archiving* (refer to page 22).
3. Configure the remote AEs which belong to the PACS that the PACS Store and Remember archive stores to and remembers from.

This step is necessary because studies can be received from a machine that belongs to the PACS and that the PACS Store and Remember archive stores to and remembers from, but that is not the store or remember AE.

Note:

For the PAP to automatically register studies as PACS archived, at least one open PACS volume must exist. When a PACS Store and Remember archive is installed, ensure that it works by storing a study to the archive, then retrieving it back from the archive.

To configure a source to send to the PAP component

1. If the source is another IMPAX system, log into the source Administration Tools.
2. On the Setup tab, select **Network Management**. 
3. Create a new station with a unique ae_title and specify the host containing the PAP and port 9104.
4. Click **Save**. 

To configure the remote AEs that belong to the PACS

1. Determine the AE titles that belong to the PACS that the PACS Store and Remember archive stores to and remembers from.
2. Ensure that the AE title matches an ae_title in the map_ae table.
3. Log into CLUI.
4. To add the entry to the map_ini table, type:

   insert into map_ini (ini_section, ini_key, ini_value) values ('<*scu_ae_title*>', '**PACS_ARCHIVE_AE_TITLES**', '<*other_ae_titles*>'**)**

   where <*scu_ae_title*> is the AE title of the machine with the SCU drive queue and <*other_ae_titles*> is the comma-separated list of AE titles (may or may not include the PACS Store and Remember store or retrieve AE).

Note:

Ensure that no spaces appear before or after commas in the comma-separated list of AE titles. Also, when configuring a PACS for mirroring using PACS Store and Remember archiving, set up each PACS with another local archive besides the PACS Store and Remember archive.

To perform other PAP configurations

1. Disable HIS verification.

   By default, the PAP is configured to perform HIS verification.
2. Change the PAP so that it routes incoming studies.

   By default, the PAP is configured to not route incoming studies.

3. Change the study status from the default 'D'.

   By default, the PAP is configured to set the study status to 'D' (Dictated) if the incoming DICOM objects do not have the study status as part of the private tags.

   Details on how to perform each step follow.

Note:

As with any database change, signal the process that the database has been updated. In CLUI, type: **signal database_updated 0 MVF_PAP**. Or, stop and restart the affected process.

To disable HIS verification

1. Log into CLUI.
2. Type:

   update mvf_scp_service set verify_incoming_data='F' where service_ref in (select service_ref from map_implements mi , map_process mp where mi.process_ref=mp.process_ref and mp.process_title='MVF_PAP')

To change the PAP so that it routes incoming studies

1. Log into CLUI.
2. Type:

   select * from map_ini where ini_section = 'MVF_PAP'
3. If the ini_key = 'DEFAULT_ROUTE_INCOMING_DATA' exists, type:

   update map_ini set ini_value = 'TRUE' where ini_section = 'MVF_PAP' and ini_key = 'DEFAULT_ROUTE_INCOMING_DATA'

   or

   If the ini_key = 'DEFAULT_ROUTE_INCOMING_DATA' does not exist, type:

   insert into map_ini (ini_section, ini_key, ini_value) values ('MVF_PAP', 'DEFAULT_ROUTE_INCOMING_DATA', 'TRUE')

To change the study status from the default 'D'

1. Log into CLUI.
2. Type:

   select * from map_ini where ini_section = 'MVF_PAP'
3. If the ini_key = 'DEFAULT_STUDY_STATUS' exists, type:

   update map_ini set ini_value = 'x' where ini_section = 'MVF_PAP' and ini_key = 'DEFAULT_STUDY_STATUS'

   or

   If the ini_key = 'DEFAULT_STUDY_STATUS' does not exist, type:

   insert into map_ini (ini_section, ini_key, ini_value) values ('MVF_PAP', 'DEFAULT_STUDY_STATUS', '<*study_status*>')

Where <*study_status*> is the status set for incoming objects without a study status as part of their private tags.

Configuring an HSM archive

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).

If using an HSM archive, ensure that the mounted location is set up properly and is ready for storage and retrieval of files before HSM starts to store to or retrieve data from the mounted location.

Tip:

Do not use mapped drives to point to the HSM directory.

By default, the location of the mount point is set to C:\hsm and the location of the subdirectory is set to archive. Update the mount point to use the full UNC path and ensure that ImpaxServerUser has read and write permissions on the mount point. Refer to "Configuring cache folder permissions for remote caches and NAS" (article ID 9106) in the Administration Tools component of the *IMPAX 6.3 Server Knowledge Base*.

To set the mount point

1. At a command prompt, type:

   cd \mvf\bin

   

   Tip:

   To get information about the tool, type **mvf_hsm_archive_add_mp.exe -?** .

2. To check the mounted location, type:

   mvf_hsm_archive_add_mp.exe -S

3. To set the mounted location and directory, type:

   mvf_hsm_archive_add_mp.exe -M <*path*> **-D** <*directory*>

   where <*path*> is the full UNC path of the mount point and <*directory*> is the subdirectory.

   For example, if hsm is a shared folder, and using the default subdirectory, type:

   mvf_hsm_archive_add_mp.exe -M "c:\hsm" -D "\archive"

Moving the VOLUMES partition for DVD archives

These instructions apply only when the MVFjdvd archive package has been installed.

To move the VOLUMES partition

1. Ensure that the MVFSQLserver package has been installed.

2. At a command prompt, type:

   cd \mvf\bin

   config-disk-image.bat <*new-image-location*>

   where <*new-image-location*> is the new location for the VOLUMES partition, for example, E:\volumes.

Configuring Scavenger

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).

If you selected and installed the Scavenger package, you must designate the source and destination Archive Servers and install and start the Scavenger service.

To designate the source and destination Archive Servers

1. At a command prompt, type:

   archive_scavenger_add_source.exe -A <*local AE title*> **-S** <*source AE title*>

   where <*local AE title*> is the AE title of the destination archive and <*source AE title*> is the AE title of the archive where the studies are copied from.

To install Scavenger as a Windows Service

1. At the command prompt type:

   mvf_archive_scavenger.exe -install

To start the Scavenger Windows Service

1. Open the Windows Services console (**Start** > **Administrative Tools** > **Services**).
2. Select **Mitra System Archive Scavenger**.
3. Select **Action** > **Start**.

or

1. Restart the computer.

IMPAX services that can write to the LOGS partition on Archive Servers and Network Gateways

When IMPAX was installed, the operational log files location is set to C:\mvf\data\logs. If you have created a separate log file partition as outlined in the *IMPAX 6.3 AS300 Installation Guide*, you may want to update the default logging location to write to that partition.

Note:

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

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

Service	Process
DICOM Service Class Provider	SCP
DICOM Service Class User	SCU
DICOM Storage Cache Manager	Autopilot
DICOM Storage Cache Server	SPFTPD
DICOM MVF Library Manager	Jukebox archive
DICOM MVF Standalone Storage	Non-jukebox archive
MVF HSM Archive	HSM archive
Mitra System Archive Scavenger	Scavenger
Mitra System Compressor	Lossy Compressor
Mitra System Task Scheduler	Task Scheduler

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

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

Note:

Not all services may exist on the server.

Updating the IMPAX Server log file locations

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

To update the IMPAX log file locations

1. Select **Start** > **Administrative Tools** > **Services**.
2. For each service to be updated:

a. Right-click the service and select **Properties**.

b. Under Service status, click **Stop**.

c. In the **Start parameters** field, type:

   -f *<full path of log file>*

   For example, **-f g:\log\mitra.log**.

d. To restart the service, under Service status, click **Start**.

e. To exit the Properties dialog, click **OK**.

Note:

You must start the service before exiting the Properties dialog; otherwise, your changes are not saved.

Creating IPSEC filters to allow access to specified hosts

The IMPAX security policy blocks some TCP ports used to communicate with hosts outside the IMPAX cluster. If you are connecting to other hosts, such as a domain controller or proxy server, create IPSEC filters to allow IMPAX to access the host. The filter allows all traffic to and from the host on all ports.

Note:

If the Application Server is installed on the same machine as the IMPAX Server, the Application Server creates the necessary filters for the domain controller.

To create a domain controller policy filter

1. Open Control Panel.
2. Select **Administrative Tools**.
3. Select **Local Security Policy**.
4. Select **IP Security Policies on Local Computer**.
5. Double-click **Impax Server Policy**.
6. In the IMPAX Server Policy Properties dialog, click **Add**.
7. Follow the Security Rule Wizard and the IP Filters Wizard, accepting the defaults except where noted in the following table. The IP Filters Wizard is launched from within the Security Rules Wizard.

To assist you in determining what selections and entries to make in each dialog, we have included examples for creating a filter for a domain controller. Substitute the appropriate information for the host you are accessing.

Wizard	Screen	Options
Security Rule Wizard	Tunnel Endpoint	1. Accept default selection, **This rule does not specify a tunnel**.
Security Rule Wizard	Network Type	1. Change to **Local area network (LAN)**.
Security Rule Wizard	Authentication Method	1. Accept the default authentication method.
Security Rule Wizard	IP Filter List	1. Click **Add.**
Security Rule Wizard	IP Filter List	1. In the **Name** field, type an appropriate name for the filter. Example: Domain Controller Filter List 2. In the **Description** field, type an appropriate description for the filter. Example: Open access to the domain controller 3. Ensure that **Use Add Wizard** is enabled. 4. Click **Add**. The IP Filter Wizard is launched.
IP Filter Wizard	IP Filter Description and Mirrored property	1. Add an appropriate description. Example: **Open Access to the Domain Controller** 2. Enable **Mirrored**.
IP Filter Wizard	IP Traffic Source	1. From the **Source** address list, select **My IP Address.**
IP Filter Wizard	IP Traffic Destination	1. From the **Destination** address list, select one of**:** • **A specific DNS Name**—If the hostname is known. • **A specific IP Address**—If the IP address is known. 2. Type the fully qualified hostname or IP address. 3. If you typed a hostname and received a security warning about creating a filter using the hostname, review the content of the message for correctness and then, to create the filter, click **Yes**.
IP Filter Wizard	IP Protocol Type	1. From the **Select a protocol type** list, accept the default selection for **Any**.
IP Filter Wizard	Completing	1. Click **Finish**.

Wizard	Screen	Options
Security Rule Wizard	IP Filter List	1. Click **OK**.
Security Rule Wizard	IP Filter List	1. Select the filter you just created. Example: Domain Controller Filter List 2. Click **Next**.
Security Rule Wizard	Filter Action	1. Select **Impax Permit Action**.

Installing and configuring Curator

If you installed Curator on an AS300 single-host server, Archive Server, or Network Gateway machine, configure Curator after installing the Application Server and performing its initial configuration. Refer to "Configuring Curator INI settings" in Chapter 2 of the *IMPAX 6.3 AS300 Configuration Guide*.

If you are installing Curator on a separate machine, or on multiple machines in a master-slave configuration, do this after installing the Application Server and performing its initial configuration, as well as after configuring all the other IMPAX Server components. Refer to the *IMPAX 6.3 Curator and CD Export Server Installation Guide*.

Troubleshooting

A

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

Cannot connect to the Administration Tools

Issues

You cannot log into the Administration Tools.

Details

Two possibilities exist for this problem:

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

Solutions

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

To stop and restart the Administration Tools service

1. On Windows 2003, select **Start** > **All Programs** > **Administrative Tools** > **Services**.

   On Windows XP, open Control Panel and select **Administrative Tools**. Select **Services**.
2. Right-click **Administration Tools Server service** and select **Restart**.

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

To modify the default port range

1. To determine which ports are in use, at a command prompt, type **netstat -a**.
2. Ports within the 1200-1270 range with a state of LISTENING do not have to be modified. If you find that the ports within that range do not have a state of LISTENING:
    a. In a text editor, open C:\mvf\java\etc\jserver.properties.
    b. Search for jmtk.rmiPortRange=1200-1270.
    c. Modify the range to suit the needs of the site.
    d. Save the modified file.

Archiving considerations

B

IMPAX supports various types of archives.

Types of archives

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

Tip:

For more details on archive functionality, refer to the Archive Server component of the *IMPAX 6.3 Server Knowledge Base*.

Supported archive configurations:

- CD-R (Compact Disk Recordable)
- DVD-R (Digital Versatile Disk Recordable)
- HSM (Hierarchical Storage Management)
- PACS Store and Remember

If you are using a jukebox archive, it must be enabled and configured to make a connection with IMPAX. Install the archive according to the manufacturer's instructions.

After following the manufacturer's instructions for setup, ensure that the archive is left powered on. During the next system restart, the IMPAX system automatically detects the archive and establishes a connection.

CD-R and DVD-R

CD-R is a small, portable, round medium used to store information in digital form. DVD-R can store much more information than CD-R using the optical disk technology.

CD-R and DVD-R archives use logical volumes. Logical volumes are valid archive locations independent of cache and media. They are not intermediate data structures used for staging data prior to burn and they cannot be manually deleted without risk of permanent data loss.

HSM archive

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

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

PACS Store and Remember

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

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

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

Glossary

A

acquisition station

Any station that sends images to IMPAX. A station must be defined as an acquisition station in the Source Manager if the station is sending original acquisition images or third-party images into the IMPAX system.

AE title

Application Entity title of a DICOM station. This is a unique identifier within the network, assigned to the station.

alias

Any common name that describes the machine or its location in the hospital.

Application Server

Intermediary server between IMPAX Client and IMPAX Server machines. LDAP, Documentation, and other Business Services reside on the Application Server.

archive

A physical device for long-term storage and retrieval, such as DVD-R, DLT, or MOD. An archive can be set up in a jukebox or non-jukebox configuration. The archive is attached to the Archive Server.

C

cache

Temporary storage area for data on a computer's local or external hard drives.

CLUI

Command Line User Interface. A command line tool to help in the service of IMPAX. CLUI allows you to execute SQL statements.

C-MOVE

An operation that allows an application entity to instruct another application entity to transfer stored SOP Instances to a third application entity using the C-STORE operation.

compression

Reduces the size of a file to save both file space and transmission time. Lossless, lossy, and wavelet are examples of compression types.

C-STORE

The mechanism used to transfer SOP Instances between application entities.

D

Database Server

Server that hosts the IMPAX (MVF) database. Can be based on SQL (AS300) or Oracle (AS3000).

DICOM

Digital Imaging and Communications in Medicine. The standard communication protocol used by a PACS, HIS, or modality to exchange information or images with other systems.

E

external PACS archive

A PACS archive that resides outside the IMPAX cluster.

H

HIS

Hospital Information System. The database used by a hospital to manage patient information and scheduling.

HIS verification

An option that forces the PACS to verify all incoming images from an acquisition station or modality against specific criteria, such as the patient ID and accession number. The PACS sends a message through the RIS Gateway to verify the criteria against what is contained in the HIS. If the criteria match, then the images can be stored permanently.

hostname

The hostname is a common alphanumeric alias for the IP address of a station.

I

image cache

Images arriving in the system and images retrieved from archive locations are stored in the image cache. These images are lossless compressed.

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.

M

master Curator

When using multiple Curators, the first Curator that runs, which owns the job queue.

MVF_SCU

A process that runs on the Network Gateway to handle store and retrieve jobs for the PACS Store and Remember archive.

N

NAS

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

Network Gateway

The Network Gateway is part of the IMPAX cluster and may be housed on its own computer or may share the same computer as the Archive and Database Servers. Essentially this is the workflow manager of the IMPAX 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.

P

PACS

A Picture Archive and Communication Systems (PACS) makes it possible to electronically store, manage, distribute, and view images.

PACS archived

A status in the IMPAX system indicating that a study is stored on an external archive using PACS Store and Remember archiving.

PACS Store and Remember archive

An IMPAX server computer set up with the PACS Store and Remember archiving functionality. Usually has Network Gateway functionality.

S

SCP

Service Class Provider. A DICOM server that receives requests from an SCU. The DICOM SCP accepts images for processing, processes find and retrieve requests, and handles storage commitment requests and replies.

SCU

Service Class User. Primarily sends DICOM requests to an SCP.

single-host configuration

A configuration in which the Database, Archive Server, and Network Gateway server components are all installed on a single server.

slave Curator

When using multiple Curators, the secondary Curators. Though the master Curator owns the job queue, PREPARE jobs are associated with the Curator that started the job.

T

TalkStation

TalkStation is voice recognition software that is integrated with IMPAX 6.3. TalkStation can convert spoken speech to typed text without having to go through a transcription phase.

U

UNC

Universal Naming Convention. A convention for identifying servers and other resources on a network. UNC uses the format \\servername\resource.

V

volume

A volume refers to the division of data on the media. If a tape has two sides, each side is referred to as a separate volume.

W

web cache

Images that have been compressed by Curator are stored in the web cache. These images are compressed using Mitra Wavelet compression to reduce their size for access over low bandwidth.

Index

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W