



ImageGrid® PACS

User Manual

Software Version 4.1



Candelis®, Inc.
9903 S Santa Monica Blvd, Suite 2101
Beverly Hills, CA 90212 (USA)
T: +1.800.800.8600 (in U.S.)
T: +1.949.852.1000 (outside U.S.)
www.candelis.com



Technical Support Contacts
Email: support@candelis.com
T: +1.800.800.8600 (in U.S.)



Authorized Representative
Emergo Europe
Westervoortsedijk 60
6827 AT Anhem
The Netherlands



IFU-001 REV 27-MAR-2026

Legal Notices, Copyright

Candelis®, ImageGrid®, and ASTRA® are registered trademarks of Candelis®, Inc.

Except as permitted under the copyright law of 1976, no part of this user guide may be reproduced in any form or by any electronic or mechanical means, including the use of information storage and retrieval systems, without permission in writing from the copyright owner.

All other trademarks and registered trademarks referenced in this document are the property of their respective owners.

Intended Use of this Document

This user manual is a reference guide detailing the software's proper installation, configuration and general usage. The screens on your monitor may vary slightly from those in this guide.

This user manual is not intended to be used as instructional material for implementing medical procedures or as a substitute for live (in-person) instruction by a trained professional.

Product Intended Use

The Candelis® Radiology Picture Archiving Communications System (PACS) is a computer-based image storage/retrieval system that stores and recalls digital images from different imaging modalities, e.g. CT, digital radiography, nuclear medicine, ultrasound, magnetic resonance imaging (MRI). Images and data can be stored, communicated, manipulated and displayed within the system or across computer networks at distributed locations. It may consist of image acquisition devices, a host computer, image archiving devices, and display stations connected by a communications network.

The ImageGrid® PACS is a system intended for professional use only.

Explanation of Symbols

The following symbols may appear on the device or product labelling:

Symbol	Explanation
	Manufacturer
	Manufacture date
	Prescription use only
	Consult operating instructions
	Caution
	Serial number
	Reference number or device model
	Compliance with the Directive 93/42/EEC as Class II device
	Device may not be thrown in the trash but must be recycled according to the European Waste Electrical and Electronic Equipment Directive

WARNINGS:

- CAUTION   Consult Dell Instructions For Use prior to installation.
- CAUTION   Consult EIZO Instructions For Use prior to installation.
- CAUTION   Consult Barco Instructions For Use prior to installation.
- CAUTION  ImageGrid Measurement Tools are for "reference only" and are not to be used for diagnostic purposes.
- CAUTION  **DO NOT** place within 1.83 meters (6 feet) of a patient or in explosive environments where flammable gases such as anesthesia or oxygen may be present.

Table of Contents

Getting started with PACS User Manual

What is new in PACS User Manual

- ImageGrid 4.1.8 Release
- ImageGrid 4.1.7 Release

Introducing PACS servers

- Hardware profiles for PACS servers
 - Tower servers
 - Direct-attached storage systems
 - Rack servers
- RAID configurations for DICOM® Standard® storage
- Turning on PACS servers
- Turning off PACS servers

Introducing PACS interfaces for system administration

- Working from PACS console interface
 - Navigating in PACS console interface
 - Configuring network interfaces
 - Configuring network interfaces using the console
 - Configuring network interfaces using a laptop or workstation
 - Creating bonded interfaces using the console
 - Pinging IP addresses using the console
 - Viewing diagnostic reports using the console
 - Connecting to technical support using the console
 - Resetting administrator password using the console
 - Initiating graceful shutdowns of PACS system using the console
- Working from PACS web interface
 - Signing in to PACS web application the first time
 - Changing user passwords
 - Opening ImageGrid® Platform
 - Signing out of PACS web application

Administration

- System
- General Settings
 - Specifying business hours
 - Updating server identification information
- Network Settings
 - Editing network interface information
 - Configuring link aggregation
 - Adding static routes
 - Editing static routes
 - Deleting static routes
 - Configuring DNS settings
 - Specifying tuning parameters
 - Blocking IP addresses
 - Blocking ranges of IP addresses
- Date and Time
 - Configuring system date and time
 - Setting time zones
 - Configuring time synchronization
- Certificates
 - Requesting new certificates
 - Committing new CA certificates
 - Viewing details of certificates
 - Importing certificates
 - Exporting certificates
 - Deleting certificates
 - Working with peer certificates
 - Working with organization certificates
 - Working with root certificates
- Web Server
 - Assigning certificates to web servers
- Proxy Settings
 - Configuring proxy server settings
- Distributed Worklist
 - Inviting PACS servers to an AE community
 - Adding AEs to an existing community
 - Removing AEs from an existing community

- Distributed Worklist
 - Transferring studies to AEs in an AE community
- Notification Service
 - Adding recipients to receive system notifications
 - Editing recipient information
 - Deleting recipient records
 - Configuring delivery methods for system messages
 - Configuring SMTP servers for system notifications
- Applications Settings
 - Configuring settings for Platform Service
 - Turning on veterinary mode
 - Configuring API for Viewer applications
- License and Registration
 - Viewing licenses
 - Updating licenses
- Security Notices
 - Searching for security notices
 - Viewing details of security notices
- Configuration Backup
 - Exporting system configuration settings
 - Importing backup configuration files
- Hardware Monitoring
 - Viewing hardware components
- Audit Trail
 - Configuring settings for archiving audit trail records
 - Configuring settings for exporting audit trail records
- Mail Service
 - Configuring mail service
 - Configuring incoming mail server
 - Configuring outgoing mail server
- Software Updates
 - Installing software updates
- Shutdown

DICOM

- Application Entities
 - Adding local application entities
 - Editing local application entity information
 - Deleting local application entities
 - Adding remote application entities
 - Editing remote application entity information
 - Verifying associations with remote AEs
 - Deleting remote application entities
- DICOM Services
 - Configuring connections with DIMSE servers
 - Configuring associations with DIMSE servers
 - Configuring services for DIMSE servers
 - Configuring per-association logging for DIMSE servers
 - Turning on trusted node updates to patient fields
- Assisted Rendering
 - Adding policies for assisted rendering
 - Editing policies for assisted rendering
 - Turning off policies for assisted rendering
 - Configuring settings for assisted rendering policies
 - Deleting policies for assisted rendering
- Routing Policies
 - Adding routing policies
 - Editing information for routing policies
 - Turning off routing policies
 - Configuring settings for routing policies
 - Deleting routing policies
- Prefetching Policies
 - Adding prefetching policies
 - Editing information for prefetching policies
 - Turning off prefetching policies
 - Configuring settings for prefetching policies
 - Querying MWL responses
 - Deleting prefetching policies
- Postfetching Policies
 - Adding postfetching policies
 - Editing information for postfetching policies
 - Turning off postfetching policies
 - Deleting postfetching policies
- Tag Morphing Policies

- Understanding tag morphing
- Applying tag morphing to studies
- Adding tag morphing policies
- Editing information for tag morphing policies
- Configuring anonymization settings for tag morphing policies
- Deleting tag morphing policies
- DICOM Mapping Policy
 - Turning on outbound DICOM mapping policies
 - Turning on inbound DICOM mapping policies
 - Resetting inbound and outbound DICOM mapping policies
- Availability Notification Policies
 - Adding policies for availability notifications
 - Editing information for availability notification policies
 - Turning off policies for availability notifications
 - Deleting policies for availability notifications
- Teaching File Policy
 - Changing default teaching file policy
 - Resetting teaching file policy
- Import Service
 - Adding import service policies
 - Editing information for import service policies
 - Configuring settings for reconciling imported studies
 - Configuring settings for storing reconciled studies
 - Configuring settings for retaining studies in worklists
 - Deleting import service policies
- Study Status
 - Configuring study status
- Transparent Proxy
 - Adding transparent proxies
 - Editing information for transparent proxies
 - Deleting transparent proxies
- RT Service
 - Configuring RT Service

HL7

- HL7 Service
 - Configuring connection settings for HL7 Service
 - Configuring settings for inbound messages for HL7 Service
 - Configuring settings for outbound messages for HL7 Service
 - Configuring settings for HL7 Service Worklist
- HL7 Peers
 - Adding HL7 peers
 - Editing information for HL7 peers
 - Turning off HL7 peers
 - Deleting HL7 peers
- HL7 Stations
 - Adding HL7 stations
 - Editing information for HL7 stations
 - Deleting HL7 stations
- HL7 Mappings
 - Adding HL7 mappings
 - Editing HL7 mappings
 - Exporting HL7 mappings
 - Replacing existing HL7 mappings by importing mappings
 - Deleting HL7 mappings
- HL7 Test Tool
 - Validating HL7 parsing messages
 - Composing and testing HL7 messages

Patient

- Quality Control
 - Configuring parameters for detecting conflicts in patient data
 - Configuring data sources for import reconciliation
 - Assigning score weights to patient demographic data
 - Turning on MWL data correction
- Identification Domain
 - Adding domains for patient identification
 - Editing information for patient identification domains
 - Configuring patient identification domains for local systems
 - Deleting patient identification domains
- Demographics Supplier
 - Turning on remote patient demographics supplier
- PIX Settings
 - Configuring PIX manager

Turning on PIX queries

ASTRA

ASTRA Service

- Configuring network settings to access ASTRA Cloud
- Turning on download redirection
- Registering PACS appliance with ASTRA Service
- Downloading private key for ASTRA Cloud
- Restoring private key for ASTRA Cloud

ASTRA Peers

- Adding ASTRA Cloud peers
- Editing information for ASTRA peers
- Deleting ASTRA peers

Users

User Management

- Changing administrator password
- Adding user accounts
- Editing information for user accounts
- Unlocking user accounts
- Deleting user accounts

Site Security Policy

- Configuring security settings for user accounts

Active Sessions

- Viewing active sessions

Data Management

Local Storage

- Managing devices and volumes
- Specifying storage types for volumes
- Configuring storage settings

ASTRA Storage

- Configuring expiration settings for ASTRA Cloud storage

Backup Service

- Turning on backup services
- Adding backup policies
- Turning off backup policies
- Editing information for backup policies
- Deleting backup policies

Data Retention

- Adding data retention policies
- Turning off policies for data retention
- Editing information for data retention policies
- Deleting backup policies

Auto Deletion

- Configuring settings for auto deletion

Storage Optimization

- Configuring settings for storage optimization
- Scheduling storage optimization services

Live Migration

- Understanding live migration
- Configuring settings for live migration
- Initiating live migration
- Tracking progress of live migration
- Deleting AEs from live migration

XDS

XDS Service

- Configuring settings for XDS service

XDS Registry

- Configuring settings for XDS registry

XDS Repository

- Configuring settings for XDS repository

Patients

Search

- Searching for existing patient records
- Searching for existing veterinary patient records
- Viewing details of patient records

Conflicts

- Searching for patient records with conflicting data
- Searching for veterinary patient records with conflicting data
- Resolving conflicts in patient data

Create Patient

- Creating patient records

- Editing information in patient records
- Merging patient records
- Exporting patient studies to CD/DVD export worklist
- Linking patient records
- Unlinking patient records
- Querying PIX manager
- Deleting patient records

CD/DVD

- Exporting patient studies to CD/DVD
- Importing studies from CD/DVD

Bulk Import

- Scanning volumes for import into PACS
- Importing scanned data into PACS

Studies

Study Search

- Searching for patient study records
- Viewing details of patient study records
- Attaching files to patient study records
- Viewing attached files from patient study records
- Deleting attached files from patient study records
- Manually changing status of patient study records
- Creating teaching files to anonymize patient study records
- Applying tag morphing policies to patient study records
- Exporting patient study records to .csv files
- Transferring studies, series, or instances
- Viewing DICOM tags associated with study instances
- Viewing structured report instances
- Downloading study records
- Editing details of study records
- Understanding study move operations
- Moving study information to patient records
- Moving series information to patient records
- Moving study instance information to patient records
- Understanding study merge operations
- Merging study records
- Merging study series records
- Deleting study, series, or instance records

Series Search

- Searching for patient study series records
- Transferring patient study series records
- Deleting patient study series records

Teaching File

- Searching for teaching file patient study records
- Working with anonymized patient study records

Requests for Priors

- Viewing patient study records listed in Requests for Priors

Reconciliation Worklist

- Reconciling patient demographics data in imported studies
- Additional system operations performed on imported studies
- Deleting studies from Reconciliation Worklist

Import Store Worklist

- Manually storing studies to local AEs
- Deleting studies from Import Store Worklist

Modality Worklist

- Viewing procedures on Local Modality Worklist
- Rescheduling procedures on Local Modality Worklist
- Deleting procedure records from Local Modality Worklist
- Viewing procedures on Remote Modality Worklist

Distributed Worklist

- Transferring studies to AEs in an AE community

Study Locks

- Manually releasing locked study records

Transfers

Routing Worklist

- Searching for routing jobs in Routing Worklist
- Viewing details of jobs in Routing Worklist
- Viewing transaction records of jobs in Routing Worklist
- Retrying failed jobs in Routing Worklist
- Rescheduling jobs in Routing Worklist
- Deleting jobs in Routing Worklist

Pre/Post Fetching Worklist

- Searching for prefetching and postfetching jobs in Pre/Post Fetching Worklist

- Viewing fetching triggered jobs in Pre/Post Fetching Worklist
- Rescheduling jobs in Pre/Post Fetching Worklist
- Deleting jobs in Pre/Post Fetching Worklist
- Backup Catalog
 - Searching for study catalog records
 - Restoring study catalog records
 - Searching for system catalog records
- Backup Worklist
 - Searching for backup job records in Backup Worklist
 - Retrying pending or failed jobs in Backup Worklist
 - Deleting failed backup jobs from Backup Worklist
- HL7 Worklist
 - Searching for HL7 messages in HL7 Worklist
 - Viewing details of HL7 messages in HL7 Worklist
 - Retrying pending or failed HL7 messages in HL7 Worklist
 - Deleting HL7 messages from HL7 Worklist
 - Exporting HL7 messages from HL7 Worklist
- ASTRA Worklist
 - Searching for ASTRA Cloud jobs in HL7 Worklist
 - Viewing details of ASTRA Cloud jobs in ASTRA Worklist
 - Retrying ASTRA Cloud jobs in ASTRA Worklist
 - Deleting ASTRA Cloud jobs from ASTRA Worklist

Reports

- Statistical Reports
 - Generating statistical reports
- Audit Trail
 - Viewing audit trail messages
- XDS Registry Objects
 - Viewing objects registered with XDS Registry
- XDS Repository Objects
 - Viewing objects stored on XDS Repository

Help & Troubleshooting

- Remote Assistance
 - Contacting Technical Support
 - Connecting to the Technical Support Center
- Diagnostic Tools
 - Performing data capture testing sessions
 - Generating diagnostic reports
- Network Tools
 - Performing network connectivity tests
- Network Activity
- Server Logs
 - Viewing logs
 - Viewing per-association logs
 - Configuring logging levels
 - Setting up remote syslog logging
- Documents

Study transfer measurements

- Theoretical study transfer rate based upon bandwidth
- Theoretical time to transfer data based on Ethernet speed
- Theoretical time to transfer data based on connection bandwidth

License agreement and warranty

- License agreement and warranty for PACS appliances utilizing software and/or hardware

Software license and warranty

Getting started with PACS User Manual

The *PACS User Manual* provides information for system administrators how to install and configure the PACS web application and for users how to perform work in the PACS web application.

The following color-coded sections are used to highlight notes and suggestions, caution or warnings, and serious errors or failure conditions.

Note

Low – Notes or suggestions.

Warning

Medium – Caution or warnings.

Danger

Major – Possible error or failure condition.

What is new in PACS User Manual

The following updates to the *PACS User Manual* support releases of the ImageGrid® PACS appliance.

ImageGrid 4.1.8 Release

- **Waiting for release notes from software engineers**

ImageGrid 4.1.7 Release

- Added topic **Direct-attached storage systems** and added Dell™ PowerVault MD2412
- In topic **Rack servers**, added Dell™ EMC PowerEdge R760XS
- Throughout, changed references of **Platform Service** to **Applications Settings**
- Added topic **Configuring API for Viewer applications**
- Throughout, deleted references to **UI Options** menu label
- In topic **Adding local application entities**, added that the list of AE Titles displays whether the AE Title is promiscuous, has read permissions, or has write permissions
- In topic **Verifying associations with remote AEs**, added step to verify TCP port address
- In topic **Adding remote application entities**, added step for selecting workarounds
- Added topic **Turning on trusted node updates to patient field**
- In topic **Adding prefetching policies**, clarified that you must select that you understand risks when selecting custom tag morphing
- In topic **Adding prefetching policies**, added information about using the Regular Expression Test Tool
- In topic **Adding prefetching policies**, added step for setting query horizon limits

Introducing PACS servers

The PACS server is a fully integrated storage and server solution that offers image archiving, image management, visualization tools, and workflow optimization capabilities for routing (pushing and pulling) images to and from workstations on the network.

Hardware profiles for PACS servers

Tower servers

The following tower servers have been used for PACS servers:

- Dell™ PowerEdge™ T300
- Dell™ PowerEdge™ T310
- Dell™ PowerEdge™ T320
- Dell™ PowerEdge™ T330

Direct-attached storage systems

The following direct-attached storage systems are supported for use with PACS servers:

- Dell™ PowerVault MD2412

Rack servers

The following rack servers have been used for PACS servers:

- Dell™ PowerEdge™ 2950
- Dell™ PowerEdge™ R510
- Dell™ PowerEdge™ R720
- Dell™ PowerEdge™ R730
- Dell™ PowerEdge™ R760XS

RAID configurations for DICOM® Standard® storage

All of the PACS server hardware models come with RAID. Starting from the T320 and R720, the RAID configurations used include RAID 1, RAID 6, and RAID 10. The configuration used will depend on the purchased configuration and the number of drives.

In older PACS servers, RAID 5 may be found.

Turning on PACS servers

Refer to the Dell user manual prior to installation.

To turn on a PACS server, perform the following steps.

1. Ensure both power cords are connected to the back of the PACS server.
2. If you have a supported UPS module, on the rear of the PACS server, use a USB cable to connect the module to an unused USB port.
3. Verify the PACS server is connected to your network, and use the network cable that was provided to you to connect to port 1 on the rear left.
4. Check each drive to make sure it is properly seated and locked in place; firmly press the drive into the chassis to ensure the latch closes.
 - All drives must be seated correctly for the PACS server to function.
 - A hard drive that is not seated properly will be considered missing or failed by the RAID controller. Depending on the RAID configuration, a few drives missing or failed will prevent the system from functioning.
5. On the front panel of the PACS server, turn on the power switch.
 - When the power supply is on, then the blue LED indicates normal operation.
 - When the LED indicator is not lit, then a power supply has failed.

Turning off PACS servers

Caution

Never turn off a PACS server by turning off the power switches or pulling the power cords. Always follow the proper shutdown procedures because a sudden or improper shutdown during heavy server activity may cause data corruption.

Introducing PACS interfaces for system administration

The PACS server provides the following interfaces for configuring and managing the PACS system.

- **Console:** Access and use the text-based console by connecting a keyboard and display to the PACS server. The console interface is most commonly used for initial setup of the system, such as configuring network interfaces; however, the console may be used to support the system.
- **Web application:** The web application includes all the features and options for configuring and managing the PACS system and is more widely used. The *PACS User Manual* focuses on how to use the web application to configure and manage the PACS server.

Working from PACS console interface

To access and use the console, connect a keyboard and a display directly to the PACS server.

- Rack-mountable servers have a VGA port and USB ports in the front and the back of the unit.
- Tower models have USB ports in the front and a VGA port and USB ports in the back.

All of the tasks that you perform in the console may also be performed from the web application.

Navigating in PACS console interface

After you connect a display to the PACS server, the first screen displays various server properties, including the model, serial number, and OS version and build.

Select **Menu** to access the following options:

- **Network Configuration** - View and manage network interfaces.
- **Ping** - Verify IP addresses and network connectivity.
- **Diagnostic Report** - Generate system data for troubleshooting issues.
- **Technical Support Connect** - Connect to technical support.
- **Shutdown** - Initiate graceful shutdown of PACS server.
- **Reset Password** - Reset the administrator password.

Use the following keys on your keyboard to move through the console screens and to select menu options:

- Arrow keys: Select menu items.
- Tab: Select a different option.
- Esc: Cancel an action or go back to a previous screen.
- Enter: Perform action for the selected option.

Configuring network interfaces

Depending on the hardware configuration, the PACS server may have two or more network interface cards (NICs), but the default configuration across systems is the same.

- **eth0:** This NIC is configured to obtain an IP address automatically through DHCP.
- **eth1:** This NIC is configured using the IP address 192.168.0.1.

After you turn on the PACS server for the first time, configure the network before proceeding. Configure the network using the following methods:

- Using the console.
- Connecting directly from a laptop or workstation to the PACS server secondary NIC using the web interface.

Configuring network interfaces using the console

To configure network interfaces from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Network Configuration**. The Network Interfaces screen displays.
3. Select the network interface that you want to configure, and then select **OK**. The Network Configuration screen displays the settings to configure.
4. Select any of the following fields, and enter the appropriate information:
 - **IP Address:** Enter a valid IP address.

- **Netmask:** Enter a valid network mask.
 - **Gateway:** Enter a default route for the network interface. Only one default gateway can be assigned to one of the network interfaces.
5. Select **Save**, and then select the **Enter** key. The settings are saved. The system restarts the network interfaces and any services that depend on the correct IP address.
 6. Open a compatible browser, and in the Address bar, enter the IP address that you assigned to the system, and then select the **Enter** key. The PACS sign-in page displays.

Configuring network interfaces using a laptop or workstation

An alternative to configuring network interfaces using the console is connecting a laptop or another workstation directly to the secondary NIC of the PACS.

To configure network interfaces using a laptop or workstation, perform the following steps.

1. Connect an Ethernet cable between the laptop and the PACS server secondary NIC. (The primary NIC should already have an Ethernet cable connecting the server to the network of the healthcare facility.)
2. From your laptop, go to **Start > Settings > Control Panel > Network Connections**. The location of the network settings depends on the operating system you are using.
3. From **Local Area Connection**, select **Properties**. The Local Area Connection Properties dialog displays.
4. Select **TCP/IP**, and then select **Properties**. The Internet Protocol Properties dialog displays.
5. Select **Use the following IP address**, and complete the following fields:
 - **IP address:** Enter *192.168.0.2*.
 - **Subnet mask:** Enter *255.255.255.0*.
6. Select **OK**.
7. Open a compatible browser, and in the Address bar, enter *192.168.0.2*, and then select the **Enter** key. The PACS sign-in page displays.

Creating bonded interfaces using the console

Combine two or more network interfaces into a single “bonded” interface to increase network performance and to add redundancy.

To create a bonded interface from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Network Configuration**. The Network Interfaces screen displays.
3. Select **Create Bond**. The Bond Configuration screen displays.
4. Select two interfaces, and then select **Create**. The Bond Configuration screen displays the settings to configure.
5. Select any of the following fields, and enter the appropriate information:
 - **IP Address:** Enter a valid IP address.
 - **Netmask:** Enter a valid network mask.
 - **Gateway:** Enter a default route for the network interface. Only one default gateway can be assigned to one of the network interfaces.
6. Select **Save**, and then select the **Enter** key. The settings are saved. The system restarts the network interfaces and any services that depend on the correct IP address.

Pinging IP addresses using the console

To ping an IP address from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Ping**. The Ping screen displays.
3. In the **IP Address** field, enter the IP address or host name that you want to ping.
4. Select **Ping**, and then select the **Enter** key. The results of the ping display.

Viewing diagnostic reports using the console

To view diagnostic information from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Diagnostic Report**. System data, such as module names and volumes, display.

Connecting to technical support using the console

Connecting to technical support requires that the PACS appliance is able to initiate a network connection to the technical support servers. Outbound connections to port 22 or port 443 must be allowed for this feature to work.

Use this feature on an as-needed basis and always with authorization and knowledge of the customer. Technical support personnel will tell you which port to use before initiating a connection.

To connect to technical support from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Technical Support Connect**. The Connect to Technical Support screen displays.
3. Complete the following fields:
 - **Address**: Enter the email address of technical support.
 - **Port**: Enter the port provided by technical support.
4. Wait for technical support to authorize and acknowledge your desire to connect.
5. Select **Connect**, and then select the **Enter** key.

Resetting administrator password using the console

The administrator (admin) is the default user for the PACS web application and other PACS system products.

To reset the administrator password from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Reset Administrator Password**. The password changes to *password*.

Initiating graceful shutdowns of PACS system using the console

To initiate a graceful shutdown of the PACS system from the console, perform the following steps.

1. From the server properties screen, select the **Enter** key. The main menu displays.
2. Select **Shutdown**. The Shutdown Options screen displays.
3. Select one of the following options:
 - **Halt**: The system remains turned off until you press the power button.
 - **Reboot**: Restart the system.
4. Select **OK**, and then select the **Enter** key. The system turns off.

Working from PACS web interface

The PACS appliance provides a web interface for managing its data and administering the system. For optimal compatibility, the following web browsers are recommended:

- Microsoft Internet Explorer Version 9 and greater
- Microsoft Edge
- Mozilla Firefox Version 11 and greater

Signing in to PACS web application the first time

The first time you sign in to the PACS web application, you have to enter contact information to identify your PACS system. This contact information may be used to send system notifications via email, establish a technical support connection, and to register with ASTRA™ Cloud services. The primary contact name that you provide should be a person who has knowledge about the PACS server and its location. The contact information will not be used for marketing purposes or shared in any way with unauthorized parties with nontechnical or service goals.

To sign in to the PACS web application the first time, perform the following steps.

1. In the Address bar of a compatible browser, enter the IP address of the system, and then press the **Enter** key. The End User License Agreement displays.
2. Read the agreement, select **I accept the terms of the license agreement**, and then select **Accept**. The PACS sign-in page displays.
3. Complete the following fields:
 - **Username**: Enter *admin*.
 - **Password**: Enter *password*.
4. Select **Sign In**. The Legal Disclaimer page displays.
5. Select the option **Don't remind me again**, and then select **Accept**. The Contact Information dialog displays.
6. Complete the following required fields:
 - **Customer Name**

- **Facility**
 - **Address**
 - **City**
 - **State/Province**
 - **Zip/Postal Code**
 - **Country**
 - **Contact Person**
 - **Contact Email**
 - **Phone Number**
7. Select **Save**. The Dashboard displays the following parts from left to right:
- **Dashboard Display** icon - Select the icon to display the default PACS dashboard.
 - **Performance Dashboard** icon - Select the icon to display just the performance statistics, such as CPU, Worklist, Network Usage, Storage Utilization, and Storage I/O Usage.
 - **Server Properties** - Displays current server properties, including whether the PACS server is registered. In the **Serial Number** field, select the **Registered** link, and the **Administration > System > License and Registration** page displays. View current licenses and update licenses.
 - **Worklist** - Displays active counts for active Worklists. Select **Transfers** from the top menu to view and manage worklists.
 - **Storage Usage** - Displays storage statistics in GB and percentages over time.
 - **System Status and Alerts** - Displays system alerts. Select the link to configure storage settings from **Administration > Data Management > Local Storage**.
 - **Platform Licenses** - Displays licenses for ImageGrid[®] Platform Viewers. View and manage all system licenses from **Administration > System > License and Registration**.
 - **CPU** - View CPU statistics.
 - **Quick Links** - Displays links to commonly used system functionality. Select a link to access the system module.
 - **Active Sessions** - Displays active sessions.
 - **Associations** - Displays local and remote associations.
 - **Network Usage** - Displays network usage statistics.

Changing user passwords

When the system prompts you that your password has expired or you want to change your password, go to the user profiles option.

Password requirements, such as required characters and required length, are configured by the local system administrator.

To change your password, perform the following steps.

1. From the top menu bar, go to **admin > Change Password**. The Change Password dialog displays.
2. In the **Current Password** field, enter your current password.
3. In the **New Password** field, enter a password.
4. In the **Re-enter Password** field, re-enter your password.
5. Select **OK**.

Opening ImageGrid[®] Platform

If you purchased a license for ImageGrid[®] Platform or an ImageGrid[®] Viewer, open the ImageGrid Platform from the PACS sign-in page to configure the environment for users of the Platform or Viewer.

You must have the Java[™] Runtime Environment (JRE) installed. The ImageGrid Platform is deployed using the Java[™] Web Start technology.

For information how to install and configure the ImageGrid[®] Platform, refer to the *ImageGrid Platform Administrator User Manual*. For information how to use the Platform, refer to the *ImageGrid Platform User Manual*.

Signing out of PACS web application

After each working session in the PACS web application, sign out of the application and close the browser.

Go to **admin > Sign Out**. The PACS sign-in page displays, and a message displays confirming you have signed out.

Administration

System

From **Administration > System**, access the following modules:

- **General Settings** - Specify business hours for your facility, and enter contact information for your system.
- **Network Settings** - Manage network settings, including interfaces, routing, DNS, and tuning parameters.
- **Date and Time** - Change system settings for date and time, time zone, and automatic time synchronization.
- **Certificates** - Configure certificate settings, including registered certificates, peer certificates, organization certificates, and root certificates.
- **Web Server** - Configure the certificate for the web server.
- **Proxy Settings** - Configure a proxy server.
- **Distributed Worklist** - Create PACS appliance communities to streamline viewing of radiology studies.
- **Notification Service** - Configure notifications to monitor system health.
- **Applications Settings** - Configure settings for client applications.
- **License and Registration** - View and update license information.
- **Security Notices** - View security notices.
- **Configuration Backup** - Create and restore system configurations.
- **Hardware Monitoring** - View the current state of hardware components.
- **Audit Trail** - Configure audit trail services.
- **Mail Service** - Configure settings for mail service.
- **Software Updates** - View the status of system software updates, and download and install updates as needed.
- **Shutdown** - Reboot or turn off a server remotely.

General Settings

Specifying business hours

From **Administration > System > General Settings**, specify typical business hours and designate whether to apply the hours to all days of the week.

The system schedules automated tasks to run outside the designated business hours. By default, business days are Monday through Friday; if your facility operates 24 hours, 7 days per week, set the business hours when the system is the most busy, and select the option to include weekends.

To specify business hours, perform the following steps.

1. Go to **Administration > System > General Settings**. The General settings pane displays the Site Settings and Server Identification sections.
2. In the Site Settings section, select the daily business hours from the following dropdown lists:
 - **Start Time** - Designate the hour and minute when the business day starts.
 - **End Time** - Designate the hour and minute when the business day ends.
 - **Include Weekends** - Select to apply the start and end times to all the days of the week.
3. Select **Save**.

Updating server identification information

From **Administration > System > General Settings**, complete the contact information that identifies your system. Technical support and IT staff may use this information to find the location of the appliance or to find the primary person or group responsible for the appliance. This contact information will also be used to send e-mail alerts, establish a support connection, and register with ASTRA™ Cloud services.

To update server identification information, perform the following steps.

1. Go to **Administration > System > General Settings**. The General settings pane displays the Site Settings and Server Identification sections.
2. In the Server Identification section, complete the following required fields:
 - **Customer Name**
 - **Facility**
 - **Address**
 - **City**
 - **State/Province**
 - **Zip/Postal Code**

- **Country**
 - **Contact Person**
 - **Contact Email**
 - **Phone Number**
3. Select **Save**.

Network Settings

From **Administration > System > Network Settings**, perform the following tasks:

- View and modify network interface information, and combine interfaces using link aggregation on the **Network Interfaces** tab.
- Add static routes to the routing table on the **Static Routes** tab.
- Configure DNS settings on the **Domain Name Service** tab.
- Adjust basic tuning parameters for network connections on the **Tuning Parameters** tab.
- Block specific IP addresses or a range of IP addresses on the **IP Blocking** tab.

Editing network interface information

From **Administration > System > Network Settings > Network Interfaces** tab, view and edit the interfaces that exist in the system.

In the **Network Interfaces** table, an interface displays a status of Connected or Disconnected, which indicates whether a cable has been connected to or disconnected from the network interface. This status does not indicate whether the interface is configured correctly.

After you edit network interface information, restart networking for the changes to take effect. Some services rely on the IP address of the system.

To edit network interface information, perform the following steps.

1. Go to **Administration > System > Network Settings**. The Network Interfaces tab displays each interface in the system.
2. In the row that includes the interface for which you want to modify information, select **Edit**. The Edit Network Interface dialog displays.
3. Modify information in the following fields. You cannot modify the interface name.
 - **Mode**: Select one of the following modes:
 - **DHCP**: System will attempt to retrieve an IP address from the DHCP server in the network to which the NIC is connected.
 - **Static**: Enter the IP address manually. Choose this option when the IP address will never change.
 - **Disabled**: Disable the network interface.
 - **IP Address**: Enter a valid IP address for the network interface.
 - **Subnet Mask**: Enter a valid subnet mask value.
 - **Gateway**: Enter the default route for the network interface. Only one gateway can be assigned to one of the network interfaces.
 - **Speed**: Select a speed. If you select Autodetect, the system automatically detects the speed.
4. Select **OK**. The changes are saved.
5. Restart the network services by selecting **Restart Networking**. The system may lose connectivity while the network restarts. If you cannot access the administration interface after one or two minutes, set the IP address by connecting a keyboard and monitor to the server and then use the console interface to set the correct IP address.

Configuring link aggregation

From **Administration > System > Network Settings > Network Interfaces** tab, configure link aggregation, which is the process of combining two or more network interfaces into a single “bonded” interface. A bond will be grouped with its bond slaves. A bond cannot be modified after it is created; it may only be deleted.

The purpose of link aggregation, also known as network interface bonding, is to increase network performance and to add redundancy. Although several types (or modes) of bonding are available, the PACS appliance currently only supports mode-4 (802.3ad). This mode is known as dynamic link aggregation, and it requires a switch that supports IEEE 802.3ad.

To use link aggregation, the following prerequisites must be met:

- The system must be a physical appliance.
- The network must have hardware support.
- At least two interfaces must be selected. The **Configure Link Aggregation** option is not available until you select two or more network interfaces on the **Network Interfaces** tab.

To configure link aggregation, perform the following steps.

1. Go to **Administration > System > Network Settings**. The Network Interfaces tab displays each interface in the system.
2. Select two or more interfaces that you want to link, and select **Configure Link Aggregation**. The Configure Link Aggregation dialog displays.
3. Complete the following fields:
 - **IP Address**: Enter a valid IP address for the network interface.
 - **Subnet Mask**: Enter a valid subnet mask value.
 - **Gateway**: Enter the default route for the network interface.
4. Select **OK**. The changes are saved.

Adding static routes

When the system is located where more than one network exists, add network routes manually. From **Administration > System > Network Settings > Static Routes** tab, add static routes.

It is recommended that a network administrator who understands the topology of the network adds static routes.

To add a static route, perform the following steps.

1. Go to **Administration > System > Network Settings > Static Routes** tab. Existing routes display.
2. Select **Add New**. The Add New Static Route dialog displays.
3. Complete the following fields:
 - **Interface**: Select the network interface that is affected by this route.
 - **Host-Only**: Select to add a static route to an individual host.
 - **Destination**: Enter the prefix of the destination network. For example, enter **192.168.10.0**. The **Destination** field is required to complete.
 - **Subnet Mask**: Enter a valid network mask. For example, enter **255.255.255.0**. If you selected **Host-Only**, this field does not display.
 - **Gateway**: Enter the IP address through which the network traffic needs to be routed.
4. Select **OK**. The changes are saved.

Editing static routes

To edit a static route, perform the following steps.

1. Go to **Administration > System > Network Settings > Static Routes** tab. Existing routes display.
2. In the row that includes the route you want to edit, select **Edit**. The Edit Static Route dialog displays.
3. Edit the information in the appropriate field, and select **OK**. The changes are saved.

Deleting static routes

To delete a static route, perform the following steps.

1. Go to **Administration > System > Network Settings > Static Routes** tab. Existing routes display.
2. In the row that includes the route you want to delete, select **Delete**. The Delete Static Route dialog displays.
3. Confirm the deletion by selecting **Yes**. The static route is removed.

Configuring DNS settings

From **Administration > System > Network Settings > Domain Name Service** tab, configure domain name service (DNS) settings.

To configure DNS settings, perform the following steps.

1. Go to **Administration > System > Network Settings > Domain Name Service** tab. Current DNS settings display.
2. Enter or modify DNS settings in any of the following fields:
 - **Host Name**: Enter the hostname of the system.
 - **Domain Name**: Enter the name of the domain in which the system is located.
 - **Search Domain Name**: Enter a local domain name that the system will use to complete unqualified hostnames (hostnames without a domain name) during DNS resolution.
 - **DNS Server 1, 2, and 3**: Enter the IP address(es) of a DNS server.
3. Select **Save**.
4. Clear the information in the DNS fields by selecting **Clear DNS**.

Specifying tuning parameters

From **Administration > System > Network Settings > Tuning Parameters** tab, specify transmission control protocol (TCP) parameters.

To specify tuning parameters, perform the following steps.

1. Go to **Administration > System > Network Settings > Tuning Parameters** tab.
2. Enter values in any of the following tuning parameter fields:
 - **Idle Connection Timeout**: Specify the number of seconds before an inactive TCP connection closes.
 - **Idle Connection Probing Frequency**: Specify the interval in seconds between scanning for idle connections.
 - **Idle Connection Probing Retries**: Specify the number of times the system retries a probe.
3. Select **Save**.

Blocking IP addresses

From **Administration > System > Network Settings > IP Blocking** tab, specify specific IP addresses for which you want to deny access to the server.

To block an IP address, perform the following steps.

1. Go to **Administration > System > Network Settings > IP Blocking** tab. The IP addresses that have been blocked display.
2. Select **Block Address**. The Block IP Address dialog displays.
3. In the **IP Address** field, enter a valid IP address, and select **OK**.

Blocking ranges of IP addresses

From **Administration > System > Network Settings > IP Blocking** tab, specify a range of IP addresses for which you want to deny access to the server.

To block a range of IP addresses, perform the following steps.

1. Go to **Administration > System > Network Settings > IP Blocking** tab. The IP addresses that have been blocked display.
2. Select **Block Range**. The Block IP Address Range dialog displays.
3. Complete the following fields:
 - **Start IP Address**: Enter a valid IP address that starts the range to block.
 - **End IP Address**: Enter a valid IP address that ends the range to block.
4. Select **OK**.

Date and Time

From **Administration > System > Date and Time**, change the system settings for date and time, time zone, and automatic time synchronization.

Configuring system date and time

The system time parameter uses the 24-hour format.

To configure date and time settings, perform the following steps.

1. Go to **Administration > System > Date and Time**. The **Date/Time** tab displays.
2. On the calendar, select the correct month and day.
3. From the **System Time** dropdown lists, select the correct hour and minutes, respectively.
4. Select **Save**.

Setting time zones

To set the system time zone, perform the following steps.

1. Go to **Administration > System > Date and Time > Time Zone** tab.
2. From the **Time Zone** dropdown list, select the correct time zone.
3. Select **Save**.

Configuring time synchronization

From **Administration > System > Date and Time > Synchronization** tab, turn on and configure time synchronization.

Time synchronization uses the network time protocol (NTP). By default, the server is configured to get the time from a server returned by `ntp.ubuntu.com`. This means that the system must be able to access the internet. Some customer sites may have their own local or internal NTP server. If you use your own server, modify the time server address.

In instances where the internal clock deviates from the network time, the software is designed to initiate an automatic synchronization. However, if the time discrepancy extends to several hours or days, the automatic synchronization feature may not activate. Under such circumstances, it is recommended to manually adjust the internal clock to closely align with the current time.

It is only recommended to turn off (clear the **Enabled** checkbox) automatic time synchronization if the site blocks external IP connections to the time server, preventing synchronization, and no local or internal time server is available. If the site blocks external IP connections to the time server and a local or internal time server is available, then it is highly recommended to change the time server address to that available server. Otherwise, over time, the clock could shift too far and deviate from the rest of the network servers.

To configure time synchronization, perform the following steps.

1. Go to **Administration > System > Date and Time > Synchronization** tab.
2. Select **Enabled** to turn on automatic time synchronization.
3. In the **Time Servers** field, enter the IP address or hostname (DNS must be set) of one or more NTP servers. Separate additional NTP server addresses with a space after each address.
4. Select **Save**.
5. Select **Synchronize**. The time synchronization process completes.

Certificates

From **Administration > System > Certificates**, manage certificates in the system by performing the following tasks:

- View existing registered certificates for the system, and request new certificates on the **My Certificates** tab.
- View certificates for remote applications or systems on the **Peer Certificates** tab.
- View intermediate certificates certified by a trusted certificate authority (CA) on the **Organization Certificates** tab.
- View all root CA certificates installed on the system on the **Root Certificates** tab.
- Import and export certificates and delete certificates from all tabs. The steps for performing these tasks are the same regardless of the type of certificate.

Requesting new certificates

From **Administration > System > Certificates > My Certificates** tab, view all the registered certificates used for the system. One default certificate is always created during system installation.

At least one certificate is required for the system, but you may use one global certificate for all the secure applications, such as the Web Service, DICOM Service, and HL7 Service. If you want to use different certificates for each application, import the certificates or request a new certificate.

When you request a new certificate, determine the type of certificate you want:

- Self-signed certificates do not require signature by a CA organization.
- CA-signed certificates require signature by a CA organization.

To request a new certificate, perform the following steps.

1. Go to **Administration > System > Certificates**. The My Certificates tab displays existing registered certificates for the system. Self-signed certificates display in the **Certificate** section, and CA certificates display in the **Certificate Signing Request** section.
2. Select **Request New**. The Request New - Certificate Type dialog displays.
3. Select the type of certificate signing method, and then select **Next**. The Request New - Private Key dialog displays. If you need to return to a previous page, select **Previous**.
4. Select the length of the private key, and then select **Next**. The Request New - Certificate Detail dialog displays.
5. Complete the following required fields:
 - **Common Name**
 - **Country**
 - **State/Province**
 - **Organization**
 - **Email Address**
 - **Valid Period (Years)**
6. Select **Next**. The Request New - Review dialog displays.

7. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Request New - Review dialog displays.
8. Review the information you entered, and select **Finish**.
 - A confirmation dialog displays.
 - A self-signed certificate is automatically signed and registered for this system, and it displays in the **Certificate** section. This certificate is also available for all the secure applications to use for secure communication; however, you need to specify the certificate on the configuration page for each application.
 - A CA certificate displays in the **Certificate Signing Request** section and requires signature by the CA organization. Refer to the procedure for Committing new CA certificates.

Committing new CA certificates

After you request a CA certificate, a Certificate Signing Request (CSR) is generated. Export the CSR file to your local drive, and then submit it to your signing authority. Refer to the procedure for Exporting certificates. Complete the certificate generation process by uploading and committing the CA certificate and intermediate CA bundle, if applicable.

To commit a CA certificate, perform the following steps.

This procedure assumes you have completed the process for obtaining a signature for the CA certificate.

1. Go to **Administration > System > Certificates > My Certificates** tab.
2. In the **Certificate Signing Request** section, select **Commit** next to the certificate you want to upload and commit. The Commit dialog displays.
3. Upload the appropriate certificate by selecting **Choose File**, selecting the file, and selecting **Open**.
4. Select **Import**. The certificate file is imported and displays in the **Certificate** section of the **My Certificates** tab.

Viewing details of certificates

From **Administration > System > Certificates**, view the details of certificates that are located on the tabs for **My Certificates**, **Peer Certificates**, **Organization Certificates**, and **Root Certificates**.

To view the details of a certificate, perform the following steps.

1. Go to **Administration > System > Certificates**, and select the tab that includes the certificate of which you want to view the details.
2. In the row that includes the certificate you want to view, select **View**. The Certificate dialog displays the **Basic** tab, which includes high-level information of the certificate.
3. View additional certificate details by selecting either of the following tabs:
 - **Detailed**: View specific details, including version and serial number.
 - **Content**: View certificate content.
4. Select **Close**. The main tab redisplay.

Importing certificates

From **Administration > System > Certificates**, import certificate files, private key files, intermediate CA certificate bundle files, CA files, and root certificate files on the tabs for **My Certificates**, **Peer Certificates**, **Organization Certificates**, and **Root Certificates**.

It is required to import a certificate file and private key file. If the certificate is generated from an intermediate certificate, you must import the intermediate CA bundle file.

To import a certificate file, perform the following steps.

1. Go to **Administration > System > Certificates**, and select the tab where you want to import a certificate file.
2. Select **Import**. The Import dialog displays options for uploading files, such as Certificate, Private Key, and Intermediate Bundle, based on the tab where you selected **Import**.
3. For the appropriate file type, select **Choose File**, select the file, and then select **Open**.
4. Select **Import**. The file is imported and displays in the list.

Exporting certificates

When you export a certificate, the files are bundled into a .zip folder that you are able to save to your local workstation.

- For a certificate, the .zip folder includes the certificate and private key files.
- For a certificate signing request, the .zip folder includes only the certificate signing request file.

From **Administration > System > Certificates**, export certificates that are located on the tabs for **My Certificates**, **Peer Certificates**, **Organization Certificates**, and **Root Certificates**.

To export a certificate, perform the following steps.

1. Go to **Administration > System > Certificates**, and select the tab from which you want to export a certificate.
2. In the row that includes the certificate you want to export, select **Export**. The files are generated and saved in a .zip folder.
3. Save the .zip folder to your local workstation as needed.

Deleting certificates

From **Administration > System > Certificates**, delete certificates that are located on the tabs for **My Certificates**, **Peer Certificates**, **Organization Certificates**, and **Root Certificates**.

To delete a certificate, perform the following steps.

1. Go to **Administration > System > Certificates**, and select the tab that includes the certificate you want to delete.
2. In the row that includes the certificate you want to delete, select **Delete**. The Delete Certificate dialog displays.
3. Confirm the deletion by selecting **Yes**. The certificate is removed.

Working with peer certificates

From **Administration > System > Certificates > Peer Certificates** tab, view all the certificates of remote applications or systems with which the local secure applications communicate. The certificates listed in this category may be referenced by DICOM remote application entities (AEs) for secure DICOM transfers or referenced by HL7 peers for secure HL7 transfers.

It is not mandatory for remote applications or systems to have registered certificates for the local secure applications to establish a secure connection with them. If both the remote certificates and the local certificates are issued from the same CA intermediate certificate and the intermediate certificate is registered in the **Organization Certificates** category, then the remote certificates do not need to be imported and registered in the **Peer Certificates** category.

From the **Peer Certificates** tab, perform the following tasks:

- [View peer certificate details.](#)
- [Import peer certificates and intermediate bundles.](#)
- [Export peer certificates.](#)
- [Delete peer certificates.](#)

Working with organization certificates

From **Administration > System > Certificates > Organization Certificates** tab, view all the trusted CA intermediate certificates registered in the system.

A peer certificate issued by a trusted CA intermediate certificate does not need to be explicitly registered to be able to establish a secure connection with this system. For example, if a certificate listed in the **My Certificates** category is issued by a CA intermediate certificate, after importing the intermediate certificate together with the certificate from the **My Certificates** category, you may also import this intermediate certificate into the **Organization Certificates** category. In this situation, all the certificates issued by this intermediate certificate are considered trusted. If a remote AE with the same intermediate certificate tries to initiate a secure DICOM connection with a local AE, then the certificate of this remote AE is not required to be listed in the **Peer Certificates** category.

From the **Organization Certificates** tab, perform the following tasks:

- [View organization certificate details.](#)
- [Import organization CA files.](#)
- [Export organization certificates.](#)
- [Delete organization certificates.](#)

Working with root certificates

From **Administration > System > Certificates > Root Certificates** tab, view all certificates that identify the root CA.

The system is installed with a default list of root certificates, but you may import additional root certificates as necessary.

From the **Root Certificates** tab, perform the following tasks:

- [View root certificate details.](#)
- [Import root certificate files.](#)
- [Export root certificates.](#)
- [Delete root certificates.](#)

Web Server

The default communication protocol used by the web server is the secure HTTPS.

Assigning certificates to web servers

From **Administration > System > Web Server**, assign a certificate to be used by the web server.

Certificates that may be assigned to the web server must be added to the **My Certificates** category from **Administration > System > Certificates**. Refer to Requesting new certificates.

To assign a certificate to the web server, perform the following steps.

1. Go to **Administration > System > Web Server**.
2. From the **Certificate** dropdown list, select the certificate to assign to the web server, and select **Save**.
3. Restart the web server for changes to take effect. Be aware that all the users will be signed out during the restart process.

Proxy Settings

Features, such as automatic software upgrades, security and firmware updates, and ASTRA services, require internet access. If internet access requires a proxy server, then add the proxy settings from **Administration > System > Proxy Settings**.

Configuring proxy server settings

From **Administration > System > Proxy Settings**, configure proxy settings for the web server.

To configure the proxy server, perform the following steps.

1. Go to **Administration > System > Proxy Settings**.
2. In the **Proxy Server** section, complete the following fields:
 - **Host Address**: Enter the IP address of the proxy server.
 - **Port**: Enter the listening port of the proxy server.
 - **Requires Authentication**: Select to designate whether the proxy server requires authentication.
3. If the proxy server requires authentication, then in the **Proxy Authentication** section, complete the following fields:
 - **Username**: Enter the username that will access the proxy server.
 - **Password**: Enter the password for accessing the proxy server.
4. Select **Save**.

Distributed Worklist

From **Administration > System > Distributed Worklist**, create a community of PACS appliance servers to streamline the process of transferring and viewing radiology studies among the AEs that are local to each PACS server in the community.

For example, a healthcare organization may have several facility locations, such as a hospital and a clinic, each with its own PACS system and its own physicians who read radiology studies. Creating a community of local AEs allows physicians to transfer patient studies from one AE to another AE in the community that is in closer proximity for ease of reading studies.

Inviting PACS servers to an AE community

From **Administration > System > Distributed Worklist > Membership** tab, create a community of PACS appliance servers by inviting other PACS servers to your community. Then from the **Community AEs** tab, each active PACS server adds its local AEs to the community.

Only one AE community can exist at a time on a PACS server, but the community may include an unlimited number of local AEs.

To invite a PACS server to an AE community, perform the following steps.

1. Go to **Administration > System > Distributed Worklist > Membership** tab. Any PACS servers that are part of the community display with the status **Active**.

2. Select **Invite**, and complete the following fields:
 - **Site Name**: Enter a descriptive name for the site or PACS system that you want to invite to the AE community.
 - **Host ID Address**: Enter a valid IP address of the PACS appliance that you want to invite to the community.
3. Select **Send**.
 - The invited PACS displays in the **Membership** list, and the **Status** field displays **Inviting**.
 - Next to the **Status** of the invited PACS, the **Accept Invite** option displays.
4. From the interface of the invited PACS, in the row that includes the invited PACS, select **Accept Invite**. The PACS server is added to the community, and the **Status** field displays **Active**.
5. Select **Refresh** to update the list of PACS in the community and the **Heartbeat** timestamp, which indicates the last time the PACS checked in and may represent whether it is accessible.

Adding AEs to an existing community

After an AE community has been created, each invited PACS server adds its local AEs to the community from **Administration > System > Distributed Worklist > Community AEs** tab. An AE must be added from **Administration > DICOM > Application Entities** before it can be added to an existing community. When an AE that is not local to your system is added to a community, then that AE title is automatically added as a remote AE to your system and displays from **Administration > DICOM > Application Entities > Remote** tab.

To add an AE to the existing AE community, perform the following steps.

1. Go to **Administration > System > Distributed Worklist > Community AEs** tab. AEs that are part of the community display. AEs that are local to your system display with a **Remove** option next to it.
2. From the AE dropdown list, select an AE, and then select **Add**. The AE displays in the **Community AEs** list with a **Remove** option next to it.
3. Select **Refresh** to update the list of AEs in the community.

Removing AEs from an existing community

From **Administration > System > Distributed Worklist > Community AEs** tab, remove a local AE from the AE community. You can only remove an AE from a community if that AE is local to your PACS appliance system. Removing an AE from the community does not remove the local AE from your system.

To remove a local AE from an existing community, perform the following steps.

1. Go to **Administration > System > Distributed Worklist > Community AEs** tab.
2. In the row that includes the local AE that you want to remove, select **Remove**. The AE is removed from the community.
3. Select **Refresh** to update the list of AEs in the community.

Distributed Worklist

From **Studies > Distributed Worklist**, view the PACS servers that are participating in an AE community, and view a list of current (unread) studies that are located on the local AEs that have been added to the existing AE community.

If an AE community has not been created, then the **Studies > Distributed Worklist** will be empty.

To create an AE community, go to **Administration > System > Distributed Worklist > Membership** tab.

Transferring studies to AEs in an AE community

From **Studies > Distributed Worklist**, send current studies to AEs in your AE community. If an AE community has not been created, then the Distributed Worklist will be empty.

If you want to transfer a study to a location, such as a remote AE or an ASTRA™ peer, that is not part of an AE community, go to **Studies > Study Search**.

To transfer a study to an AE in your AE community, perform the following steps.

1. Go to **Studies > Distributed Worklist**. The PACS servers that are part of the AE community display.
2. Expand the list of studies to find the study that you want to transfer to an AE in the community.
3. Select the row of the study, and from the **Transfer** dropdown list, select the AE to which to transfer the study, and then select **Send**.

View the studies from an image viewer.

Notification Service

From **Administration > System > Notification Service**, manage methods for delivering system messages and maintain recipient records by performing the following tasks:

- Add users who need to receive system notifications, and modify and delete recipient records on the **Recipients** tab.
- Specify message delivery methods on the **Configuration** tab.
- Configure an SMTP server on the **SMTP Server** tab.

The PACS appliance provides two separate mechanisms for delivering system notifications to users. The system can either be configured to send email messages and/or SMS notifications through the Candelis ASTRA™ Cloud-based service or to send email notifications only by connecting directly to an external SMTP server.

To turn on ASTRA notifications, the system must be licensed and registered with ASTRA. To prevent unnecessary or unintended spamming, notifications must also be turned on for the registered account. Contact your sales representative or technical support for more information.

Adding recipients to receive system notifications

From **Administration > System > Notification Service > Recipients** tab, add users who need to receive system notifications, which are grouped by topic, such as system administration, connectivity, and routing. For each recipient, assign a severity to a topic notification, which means the user receives notifications that meet or exceed that severity.

To add a recipient, perform the following steps.

1. Go to **Administration > System > Notification Service**. The Recipients tab displays a list of recipients.
2. Select **Add Recipient**. The Add New Recipient dialog displays.
3. Complete the following required fields:
 - **Name**: Enter the name of the recipient.
 - **Email Address**: Enter a valid email address for the recipient.
 - **Phone Number**: Enter a valid phone number for the recipient. A phone number is only required when SMS is configured.
4. In the **Severity** column dropdown list, select the severity for each notification topic.
5. In the **Email** column, select whether a topic notification is delivered to the recipient via email message.
6. (Optional) In the **SMS** column, select whether a topic notification is delivered via SMS.
7. Select **OK**. The recipient information is saved.

Editing recipient information

From **Administration > System > Notification Service > Recipients** tab, edit recipient information.

To edit recipient information, perform the following steps.

1. Go to **Administration > System > Notification Service**. The Recipients tab displays a list of recipients.
2. In the row that includes the recipient record that you want to edit, select **Edit**. The Edit Recipient dialog displays.
3. Modify the information in any of the recipient fields or **Topic** information in the **Severity** column or **Email** column.
4. Select **OK**. The recipient information is saved.

Deleting recipient records

To delete recipient records, perform the following steps.

1. Go to **Administration > System > Notification Service**. The Recipients tab displays a list of recipients.
2. In the row that includes the recipient record that you want to delete, select **Delete**. The Delete Recipient dialog displays.
3. Confirm the deletion, and select **Yes**. The record is removed.

Configuring delivery methods for system messages

From **Administration > System > Notification Service > Configuration** tab, configure delivery methods for sending system messages to recipients.

To configure delivery methods, perform the following steps.

1. Go to **Administration > System > Notification Service > Configuration** tab.
2. From the **Delivery Method** dropdown list, select the desired delivery method, and select **Save**.

Configuring SMTP servers for system notifications

From **Administration > System > Notification Service > SMTP Server** tab, configure an SMTP server.

Most external SMTP servers require the system to have a dedicated email account to send outbound notifications. Contact your mail service provider to ensure the system has the proper credentials.

To configure the SMTP server, perform the following steps.

1. Go to **Administration > System > Notification Service > SMTP Server** tab, and complete the following fields:
 - **Host Address:** Enter a valid host address for the SMTP server.
 - **Port:** Enter the listening port for the SMTP server.
 - **Username:** Enter the username for the email account used to connect to the SMTP server.
 - **Password:** Enter the password for the email account used to connect to the SMTP server.
 - **Email Sender:** Enter an email address that will display for recipients of the email messages.
 - **Use SSL/TLS:** Select to use a secure connection when connecting to the SMTP server.
2. Select **Save**.
3. Clear the information in the fields by selecting **Reset**.
4. Send a test email message by selecting **Send Test Email**.

Applications Settings

From **Administration > System > Applications Settings**, configure the general and remote access settings for the Platform Service, turn on veterinary mode, and configure the Viewer application API.

Configuring settings for Platform Service

From **Administration > System > Applications Settings > ImageGrid Platform Service** tab, configure the general and remote access settings for the Platform Service.

Consider the following when working with the listening interface:

- The listening interface will be updated automatically if it is or becomes part of a bonded interface.
- If the Platform Service is listening on an interface and that interface is used to create a bonded interface, then the setting will be changed automatically.
- If the Platform Service is listening on a bonding interface and that interface is destroyed, then the setting will be changed automatically to **All (0.0.0.0)**.

Saving changes to Platform Service settings requires restarting the Platform Service. This restart will automatically sign out all users of the viewer or RIS. Studies that are downloaded to workstations will need to be downloaded again.

To configure Platform Service settings, perform the following steps.

1. Go to **Administration > System > Applications Settings**. The ImageGrid Platform Service tab displays.
2. In the **General Settings** section, from the **Listening Interface** dropdown list, select the interface where the service will be listening for incoming connections.
3. In the **Remote Access Settings** section, complete the following fields:
 - **Allow Remote Access:** Select to allow access to the Platform products for remote users, such as referring physician viewers.
 - **External Port:** Enter the port that is reachable from the public side of an organization firewall.
 - **External IP Address:** Enter the IP address that is reachable from the public side of an organization firewall.
4. Select **Save**. The Save Settings and Restart Platform Service dialog displays.
5. Confirm that you want to restart the Platform Service, and select **Yes**.

Turning on veterinary mode

From **Administration > System > Applications Settings > Web Administration Options** tab, turn on veterinary mode to display veterinary-specific fields in search results and other information for patients and study records. When veterinary mode is turned on, users must sign out of the system, and then sign in to see the changes.

To turn on veterinary mode, perform the following steps.

1. Go to **Administration > System > Applications Settings > Web Administration Options** tab.
2. Select **Enable Veterinary Mode**, and then select **Save**. A message displays confirming the configuration changes are saved.

Configuring API for Viewer applications

From **Administration > System > Applications Settings > API Configuration** tab, configure which Viewer application, such as ImageGrid Universal Platform Viewer or ImageGrid Universal Viewer, displays when users sign in to a Viewer application.

1. Go to **Administration > System > Applications Settings > API Configuration** tab.
2. From the **Viewer Application** dropdown list, select the Viewer to display when users sign in to a Viewer application.
3. Select **Save**. A message displays confirming the API configuration changes are saved.

License and Registration

From **Administration > System > License and Registration**, view and update license information.

Physical appliances are shipped to customers pre-installed and licensed, but virtual systems that are installed by customers require a license before use. When customers purchase new licensable features or when other licensable items require a change, a new license is needed. The following methods are used to obtain the license file.

- If the system has access to the internet, the license will be available on the software upgrade server at upgrade.candelis.com. Customers are able to check whether the license is available and download it automatically.
 - If the system does not have access to the internet, tech support provides a license file via email to customers. Customers are able to upload the license file, save the license file locally, and then upload the license.

Viewing licenses

The **View License** tab displays license information, such as system model, serial number, and the unique device identifier (UDI). If no license information displays, contact technical support.

To view license information, perform the following steps.

1. Go to **Administration > System > License and Registration**. The **View License** tab displays the specific license information.
2. Filter the license items that display by entering some text in the **Filter** field.

Updating licenses

From the **Update License** tab, change or update the license. For example, if your software has been updated, then you need to upload a new license file.

To update a license for a system with internet access, perform the following steps.

1. Go to **Administration > System > License and Registration > Update License** tab.
2. Select **Get New License**. The system checks the upgrade server for an available license and automatically downloads the license.

To update a license for a system without internet access, perform the following steps.

The following steps assume that you have already received a license file from technical support and that you have saved the license file to your local system.

1. Go to **Administration > System > License and Registration > Update License** tab.
2. Select **Choose File**, browse to the license file that you saved locally, and select **Open**.
3. Select **Update**. The system automatically uploads the license. Some services will be restarted for the changes to take effect.

Security Notices

From **Administration > System > Security Notices**, view the list of common vulnerability exposures (CVE) that are addressed by the security updates currently installed on the server. Security updates are provided monthly (or as needed) at the software repository located at upgrade.candelis.com.

When a security patch is applied to the system, its CVE number is recorded in the database, enabling you to search for security notices by the CVE number.

Searching for security notices

To search for security notices, perform the following steps.

1. Go to **Administration > System > Security Notices**. The list of security notices displays by CVE number.
2. In the **Search** field, enter a specific or partial CVE number or filter term, and then select **Search**. The results that match your search display.
3. Browse through the list of notices by performing any of the following tasks:
 - Go to a specific page of results by selecting the page number from the **Page** dropdown list.
 - Go to the previous or next page of results by selecting the corresponding arrow next to the **Page** dropdown list.
4. Clear a search or filter term by selecting **Clear**.

Viewing details of security notices

To view details of a security notice, perform the following steps.

1. Go to **Administration > System > Security Notices**, and search for a security notice. The results that match your search display.
2. In the row that includes the notice of which you want to view the details, select the corresponding link in the **Reference** column. The notice opens in a separate webpage.

Configuration Backup

From **Administration > System > Configuration Backup**, create and restore the system configuration, including, but not limited to, the following settings:

- System network settings
- DICOM settings and application entities
- Routing/prefetching/postfetching policies
- HL7 peers and data mappings
- ASTRA peers
- Archive and backup settings

Exporting system configuration settings

From **Administration > System > Configuration Backup > Export Configuration** tab, export current configuration settings.

The configuration backup mechanism is specific both to the version of the PACS appliance software present on the system and to the current configuration settings. To ensure ongoing compatibility of the configuration backup, it should be performed immediately after either an upgrade (to a later version of the PACS appliance software) or subsequent to any changes to the configuration settings. Note that neither patient data nor study data are exported as part of the configuration backup.

To export the configuration settings, perform the following steps.

1. Go to **Administration > System > Configuration Backup**. The **Export Configuration** tab displays.
2. Select **Export**. The configuration information is generated and automatically downloaded to your computer.

Importing backup configuration files

From **Administration > System > Configuration Backup > Import Configuration** tab, import a backup configuration file.

Only a configuration backup from the same version of this PACS appliance should be used for restoring configuration settings. Importing an invalid configuration may result in incorrect system behavior.

To import a backup configuration file, perform the following steps.

1. Go to **Administration > System > Configuration Backup > Import Configuration** tab.
2. Select **Choose File**, select the file, and then select **Open**.
3. Select **Import**. The configuration file is imported. Some of the services will restart for the changes to take effect.

Hardware Monitoring

The PACS appliance software can be installed either on a physical hardware (an appliance) or on a virtual machine.

When the product software is installed on a physical appliance, go to **Administration > System > Hardware Monitoring** to view the current state of various hardware components. When the product software is installed on a virtual machine, hardware monitoring is not available, and the **Hardware Monitoring** module does not display.

Viewing hardware components

To view hardware components on a physical appliance, perform the following steps.

1. Go to **Administration > System > Hardware Monitoring**.
2. View hardware information by selecting one of the following tabs:
 - **Sensors**: View temperature, fan speed, and the status of power supplies.
 - **RAID Device**: View the current state of the RAID controller(s), virtual disks, and physical drives.
 - **UPS Device**: Only available on certain models. View basic UPS values obtained from a UPS connected through USB to the server.

Audit Trail

From **Administration > System > Audit Trail**, configure the settings for archiving and exporting audit trail records.

Configuring settings for archiving audit trail records

From **Administration > System > Audit Trail > Archive** tab, determine when audit trail records are automatically archived.

To configure settings for archiving audit trail records, perform the following steps.

1. Go to **Administration > System > Audit Trail**. The **Archive** tab displays.
2. Complete the following fields:
 - **Auto Archive Trigger Threshold**: Enter a threshold value that when the number of online audit records exceeds this value, the audit trail archive operation will start at midnight.
 - **Minimum Online Count**: Enter the number of audit records to be retained online.
3. Select **Save**. A message displays confirming the configuration is saved.

Configuring settings for exporting audit trail records

From **Administration > System > Audit Trail > Remote Syslog** tab, configure settings for exporting audit trail records to a remote system using the standard syslog protocol.

To configure settings for exporting audit trail records, perform the following steps.

1. Go to **Administration > System > Audit Trail > Remote Syslog** tab.
2. Complete the following fields:
 - **Enable**: Select to turn on the audit trail syslog export service.
 - **Transport Mechanism**: Select the syslog protocol, such as UDP, TCP, or TLS 1.2.
 - **Remote Syslog Host**: Enter a valid IP address of the remote syslog server.
 - **Remote Syslog Port**: Enter a valid port number of the remote syslog server.
 - **Secure Transfer Certificate**: If TLS 1.2 is selected as the transport mechanism, then select a certificate for the local syslog client. The certificate must be added from **Administration > Certificates > My Certificates** category.
 - **Record Submission Policy**: Choose whether to submit audit trail messages in batches at scheduled times or in real time. Selecting the real-time submission option may impact performance of the system.
 - **Scheduled Time**: Select the time when the audit trail export starts on the scheduled days.
 - **Scheduled Days**: Select one or more days when the audit trail export is active.
3. Select **Save**. A message displays confirming the configuration is saved.
4. Clear the archive configuration settings by selecting **Reset**.

Mail Service

From **Administration > System > Mail Service**, configure settings for incoming and outgoing mail service.

Configuring mail service

To configure the mail service, perform the following steps.

1. Go to **Administration > System > Mail Service**. The **Configuration** tab displays.
2. In the **Digital Signatures** section, configure digital signatures by completing the following fields:
 - **Enable**: Select to turn on digital signatures.
 - **My Certificate**: Select a certificate for the digital signature. The certificate must be added from **Administration > Certificates > My Certificates** category.
 - **Digest Algorithm**: Select the algorithm to use.
3. In the **Encryption** section, configure encryption by completing the following fields:
 - **Enable**: Select to turn on encryption.
 - **My Certificate**: Select a certificate for the encryption. The certificate must be added from **Administration > Certificates > My Certificates** category.

- **Peer Certificate:** Select a peer certificate. The certificate must be added from **Administration > Certificates > Peer Certificates** category.
 - **Encryption Algorithm:** Select the encryption algorithm to use.
4. In the **Return Receipts** section, configure mail receipt notifications by completing the following fields:
 - **Enable:** Select to turn on return receipts.
 - **When Sending Mail:** Select whether to never request or always request a receipt when sending mail.
 - **When Receiving Mail:** Select whether to never send or always send a return receipt when receiving mail.
 5. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring incoming mail server

To configure the incoming mail server, perform the following steps.

1. Go to **Administration > System > Mail Service > Incoming Mail Server** tab.
2. Complete the following fields:
 - **Protocol:** Enter the protocol, such as POP or SMTP, used for the mail service.
 - **Host Name:** Enter the hostname of the incoming mail server.
 - **Port:** Enter the listening port for the incoming mail server.
 - **Username:** Enter the username for the email account used to connect to the incoming mail server.
 - **Password:** Enter the password used to access the incoming mail server.
 - **Security:** Enter the security service, such as SSL/TSL, used for the incoming mail server.
3. Select **Save**. A message displays confirming the configuration changes are saved.
4. Clear the configuration settings by selecting **Clear**.

Configuring outgoing mail server

To configure the outgoing mail server, perform the following steps.

1. Go to **Administration > System > Mail Service > Outgoing Mail Server** tab.
2. Complete the following fields:
 - **Protocol:** Enter the protocol, such as POP or SMTP, used for the mail service.
 - **Host Name:** Enter the hostname of the outgoing mail server.
 - **Port:** Enter the listening port for the outgoing mail server.
 - **Username:** Enter the username for the email account used to connect to the outgoing mail server.
 - **Password:** Enter the password used to access the outgoing mail server.
 - **Security:** Enter the security service, such as SSL/TSL, used for the outgoing mail server.
3. Select **Save**. A message displays confirming the configuration changes are saved.
4. Clear the configuration settings by selecting **Clear**.

Software Updates

From **Administration > System > Software Updates**, view the status of software updates on your system, and download and install available updates.

Installing software updates

When the system is up to date, the options to **Download Updates** and **Install Updates** are not available to select.

To install software updates, perform the following steps.

1. Go to **Administration > System > Software Updates**. The **Status** tab displays the current status of software updates available for download.
2. Select **Download Updates**. The Download Updates dialog displays.
3. From the dropdown list, select the type of update you want to install, and then select **OK**. A message displays confirming that updates have been downloaded and are ready to be installed.
4. Select **Install Updates**. The Install Updates dialog displays.
5. Select when you want the updates to be installed, and select **OK**. The updates install based on your selection.

Shutdown

From **Administration > System > Shutdown**, remotely reboot or turn off the system remotely by selecting one of the following options:

- **Reboot:** Reboot the system.
- **Shutdown:** Turn off the system.

DICOM

DICOM[®] (Digital Imaging and Communications in Medicine) is the international standard for medical images and related information. It defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use.

From **Administration > DICOM**, access the following modules:

- **Application Entities** - Define and maintain local and remote application entities (AEs).
- **DICOM Services** - Configure DIMSE server settings for the DICOM Service.
- **Assisted Rendering** - Define and maintain policies for assisted rendering.
- **Routing Policies** - Define and maintain policies for routing incoming studies to other remote AEs.
- **Prefetching Policies** - Define and maintain prefetching policies, and configure the settings for prefetching jobs.
- **Postfetching Policies** - Define and maintain postfetching policies.
- **Tag Morphing Policies** - Define and maintain tag morphing policies, and configure settings for anonymization.
- **DICOM Mapping Policy** - Define inbound and outbound DICOM mapping policies.
- **Availability Notification Policies** - Define and maintain policies for availability notifications.
- **Teaching File Policy** - Change the default teaching file policy.
- **Import Service** - Define and maintain study import policies, and configure settings for the import jobs.
- **Study Status** - Configure a default status for incoming studies.
- **Transparent Proxy** - Define and maintain transparent proxies.
- **RT Service** - Configure the Radiation Therapy (RT) Service.

Application Entities

An application entity (AE) identifies a DICOM-compliant resource that can connect with and exchange images with the PACS appliance server. DICOM[®] entities include modalities, such as EMR and RIS systems, and PACS systems. The PACS appliance server can accommodate multiple local AE titles that can be used to isolate the storage of DICOM studies received from modalities or other PACS systems. For the PACS appliance server to communicate with other AEs on the network, the administrator must define a remote AE for each.

From **Administration > DICOM > Application Entities**, maintain both local and remote AEs by performing the following tasks.

- View, add, and edit local AEs on the **Local** tab.
- View, add, edit, and verify AE associations on the **Remote** tab.

Adding local application entities

From **Administration > DICOM > Application Entities > Local** tab, add local application entities (AEs). An application entity has an application entity title (AET), IP address, and port for DICOM communication.

Filter the list of local AEs by entering a term in the **Filter** field. The **Local** tab displays whether the AE title is promiscuous, has read permissions, and/or has write permissions.

To add a local AE, perform the following steps.

1. Go to **Administration > DICOM > Application Entities**. The **Local** tab displays.
2. Select **Add New**. The Local AE - Configuration dialog displays.
3. Complete the following fields:
 - **AE Title**: Enter a name that will identify this DICOM application to other DICOM applications on the network.
 - **Description**: Enter a brief description of the AE.
4. Select **Next**. The Local AE - Permissions dialog displays. If you need to return to a previous page, select **Previous**.
5. Determine which application entities can access the studies currently stored in the local application entity by selecting one of the following options:
 - **Enable Promiscuous Mode**: Select to accept associations from any remote AE regardless of whether the AE is registered with the ImageGrid.
 - **Enable Peer Access Mode**: Select to accept associations only from registered remote AEs.
 - **Read Permission/Write Permission**: If neither promiscuous mode nor peer access mode is turned on, then grant read and write access to specific registered remote AEs by adding and removing access manually.
6. Select **Next**. The Local AE - Study Deletion dialog displays.
7. Select **Allow Delete Operations** to allow studies to be deleted from this local AE, and then select **Next**. The Local AE - Advanced dialog displays.
8. From the **Peer for Prior Exchange Workflow** dropdown list, select the local AE peer for priors exchange. This option supports the viewer workflow states across peers. If this option is not configured, the viewer workflow will only work locally.

9. Select **Next**. The Local AE - Summary dialog displays.
10. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Local AE - Summary dialog displays.
11. Review the configuration, and select **Finish**. A message displays confirming the addition of the local AE.

Editing local application entity information

From **Administration > DICOM > Application Entities > Local** tab, edit local AE information.

Filter the list of local AEs by entering a term in the **Filter** field.

To edit local AE information, perform the following steps.

1. Go to **Administration > DICOM > Application Entities**. The **Local** tab displays.
2. In the row that includes the local AE that you want to edit, select **Edit**. The Local AE - Configuration dialog displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Local AE - Summary dialog displays.
4. Review the configuration, and select **Finish**. A message displays confirming the changes are saved.

Deleting local application entities

From **Administration > DICOM > Application Entities > Local** tab, delete a local AE.

To delete an existing local AE, perform the following steps.

1. Go to **Administration > DICOM > Application Entities**. The **Local** tab displays.
2. In the row that includes the local AE that you want to delete, select **Delete**. The Delete Local AE dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the deletion.

Adding remote application entities

From **Administration > DICOM > Application Entities > Remote** tab, add remote application entities (AEs).

Filter the list of remote AEs by entering a term in the **Filter** field.

To add a remote AE, perform the following steps.

1. Go to **Administration > DICOM > Application Entities > Remote** tab.
2. Select **Add New**. The Remote AE - Configuration dialog displays.
3. Complete the following fields:
 - **AE Title**: Enter a name that will identify this DICOM application to other DICOM applications on the network.
 - **Description**: Enter a brief description of the AE.
 - **Address**: Enter a valid host address for the remote AE.
 - **Port**: Enter a valid listening port for the remote AE.
 - **Peer Type**: Select the peer type.
4. Select **Next**. The Remote AE - Association Options dialog displays. If you need to return to a previous page, select **Previous**.
5. Configure the following association options:
 - **Calling AE Title**: Select the local AE to use as the calling AE title for DICOM associations to the remote AE being configured.
 - **Jobs processing**: Select the number of concurrent routing and fetching jobs per route where the remote AE is the destination. A route is a pair of one local AE and one remote AE. The highest number may not yield best performance; increase the number gradually and evaluate according to your environment, image types, network bandwidth and latency, hardware specifications, and peer capabilities.
 - **Transfers**: Select **Enable Secure Transfer** to turn on secure connections, and then from **Secure Transfer Certificate**, select a certificate for this remote AE that was added from **Administration > System > Certificates > Peer Certificates** category.
6. Select **Next**. The Remote AE - Error Handling dialog displays.
7. In the **DIMSE Status Code** field, enter the code, select **Add**, and then select **Next**. The Remote AE - Transfer Syntax dialog displays.
8. Select **Use Encapsulated Transfer Syntax** to turn on encapsulated transfer syntaxes, and then select **Next**. If turned on, the remote AE will be able to send and receive compressed and uncompressed images. If the option is not turned on, only uncompressed images will be allowed. The Remote AE - Patient Identification Domain dialog displays.
9. From the dropdown list, select the default patient identification domain that is associated with this remote AE, and then select **Next**. The Remote AE - Trusted Node dialog displays.

10. Select **Enable Trusted Node** to configure this remote AE as a trusted node, and then select **Next**. If turned on, the remote AE can overwrite existing patient demographic information in the database based on the latest image received. The Remote AE - Availability Sensing dialog displays.
11. Select **Enable Availability Sensing** to turn on availability sensing for this remote AE, and then select **Next**. If turned on, the PACS appliance may periodically send C-ECHO requests to the remote AE to check on its availability. The Remote AE - Storage Commitment dialog displays.
12. Select **Enable Storage Commitment** to send a storage commitment request to this remote AE when studies are stored to it, and then select **Next**. The Remote AE - Ignored SOP Classes dialog displays.
13. Specify SOP classes that the remote AE should ignore, and then select **Next**. The Remote AE - Workarounds dialog displays.
14. In the **Workaround** column, select the appropriate workaround to address issues, such as asynchronous C-MOVE operations, that may exist for a remote AE, and then select **Next**. The Remote AE - Summary dialog displays.
15. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Remote AE - Summary dialog displays.
16. Review the configuration, and select **Finish**.

Editing remote application entity information

From **Administration > DICOM > Application Entities > Remote** tab, edit remote AE information.

Filter the list of remote AEs by entering a term in the **Filter** field.

To edit remote AE information, perform the following steps.

1. Go to **Administration > DICOM > Application Entities > Remote** tab.
2. In the row that includes the remote AE that you want to edit, select **Edit**. The Remote AE - Configuration dialog displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Remote AE - Summary dialog displays.
4. Review the configuration, and select **Finish**. A message displays confirming the changes are saved.

Verifying associations with remote AEs

From **Administration > DICOM > Application Entities > Remote** tab, verify that associations with a remote AE can be created and that the server port is correct.

To verify an association with the remote AE, perform the following steps.

1. Go to **Administration > DICOM > Application Entities > Remote** tab.
2. In the row that includes the remote AE for which you want to verify an association, select **Ping**. The Verify Remote AE Connectivity dialog displays.
3. Verify network connectivity by selecting **Send** next to the AE.
 - Succeeded displays when an association was established, and both systems can communicate with each other.
 - Failed displays when an association was not established.
4. Verify a TCP port address is correct by selecting **Verify**.
5. Select **Close**.
6. (Optional) If the DICOM ping failed, one of the following issues may be the cause:
 - Wrong network IP address or port is configured. Verify your network settings, and check the remote AE configuration on the PACS appliance.
 - Peer is behind a firewall that is blocking the attempt to connect. Contact your network administrator to open the appropriate ports.
 - PACS appliance is unknown to the peer. Register the PACS appliance with the peer.
 - Services on the peer are not running or are having problems. Contact technical support.
 - PACS appliance and the peer are located on different networks, and no route exists between them. Contact your network administrator.
 - Peer is not a DICOM-compliant device.
 - In certain cases, a DICOM ping will succeed, but the regular ping (ICMP) will fail. This indicates that the peer is reachable, but only accepts DICOM communications.

Deleting remote application entities

From **Administration > DICOM > Application Entities > Remote** tab, delete a remote AE.

To delete an existing remote AE, perform the following steps.

1. Go to **Administration > DICOM > Application Entities > Remote** tab.
2. In the row that includes the remote AE that you want to delete, select **Delete**. The Delete Remote AE dialog displays.

3. Confirm the deletion, and select **Yes**. A message displays confirming the deletion.

DICOM Services

From **Administration > DICOM > DICOM Services**, configure the following DIMSE server settings:

- Connections
- Associations
- Services
- Per-association logging
- Updates to patient fields

Configuring connections with DIMSE servers

To configure connections with the DIMSE server, perform the following steps.

1. Go to **Administration > DICOM > DICOM Services > Connection Settings** section.
2. Complete the following fields:
 - **Listening Port**: Enter a valid inbound port for DICOM[®] associations. By default, the DICOM Service listens to incoming connections on port 104.
 - **Secure Listening Port**: Enter a valid inbound port for secure DICOM associations.
 - **Secure Transfer Certificate**: Select a certificate that was added from **Administration > System > Certificates > Peer Certificates** category.
 - **Maximum PDU Size**: Select the maximum data packet size in bytes for transferring studies to other systems across the network.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring associations with DIMSE servers

To configure associations with the DIMSE server, perform the following steps.

1. Go to **Administration > DICOM > DICOM Services > Association Settings** section.
2. Complete the following fields:
 - **Maximum Inbound Associations**: Enter the maximum number of inbound associations that may be active at any given time.
 - **Idle Association Timeout**: Select **None**, or enter a number for the amount of time in seconds before an idle association is released by the system.
 - **SCU Proposed Role**: Select the role to be proposed for DICOM associations when the system is acting as a service class user (SCU).
 - **SCP Proposed Role**: Select the role to be proposed for DICOM associations when the system is acting as a service class provider (SCP).
3. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring services for DIMSE servers

To configure services for the DIMSE server, perform the following steps.

Because some modalities do not correctly handle certain types of responses when duplicate studies are received, it is recommended that the **Duplicate Image Handling Policy** be set to **Overwrite, Success** to avoid any problems with these modalities.

1. Go to **Administration > DICOM > DICOM Services > Service Configuration** section.
2. Complete the following fields:
 - **Default Character Encoding**: Select the default character encoding used to handle associations. This setting only applies when the character set is not explicitly specified in the DICOM dataset.
 - **Duplicate Image Handling Policy**: Select one of the following action and response options that the system should take when duplicate studies are received:
 - **Reject**: No duplicate images are allowed. The system returns an error upon receiving a duplicate SOP instance UID.
 - **Overwrite, Success**: Duplicate images overwrite old instances; the server always reports a success to the sender.
 - **Overwrite, Warning**: Duplicate images overwrite old instances; the server always responds to the sender with a warning.
 - **Ignore, Warning**: Duplicate images are ignored and discarded; the server always responds to the sender with a warning.

- **Accept Unprocessable Syntaxes:** Select to allow images with unprocessable transfer syntaxes, such as MPEG2, to be accepted and stored.
 - **Send Study Status:** Select to include the study status when transferring studies to other PACS appliances and compatible systems.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring per-association logging for DIMSE servers

To configure per-association logging for the DIMSE server, perform the following steps.

1. Go to **Administration > DICOM > DICOM Services > Per-Association Logging** section.
2. Complete the following fields:
 - **Enable:** Select to log messages to individual files per association. Note that only the DICOM Service, MWL Tracker, and Routing/Fetching Service are capable of generating per-association logs; all services will continue writing to their default log files.
 - **Keep Logs:** Enter the number of days to keep per-association logs on the file system.
 - **Log Level:** Select the logging level to use when writing to per-association logs.
 - **Remote AE Titles:** Select whether to turn on per-association logs for all remote AE titles or only for specific AE titles.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Turning on trusted node updates to patient fields

By default, records that have patient data conflicts with existing patient records are not automatically updated. When you turn on the trusted node update option, then patient records that have patient data conflicts with existing records will be edited and accepted into the PACS system.

To turn on trusted node updates to patient fields, complete the following steps.

1. Go to **Administration > DICOM > DICOM Services > Advanced** section.
2. Select **Enable Trusted Node Updates to Patient Fields**.
3. Select **Save**. A message displays confirming the configuration changes are saved. Patient records that have patient data conflicts with existing records are edited and accepted into the PACS system.

Assisted Rendering

From **Administration > DICOM > Assisted Rendering**, define and maintain policies for how the PACS appliance will render DICOM images that are sent to the system. Based on the defined assisted rendering policies, the PACS server renders the raw images before they are available in the image viewer. With this process, the image viewer is downloading the pre-rendered images, which saves workstation CPU resources and shortens the image processing time for the user.

Adding policies for assisted rendering

From **Administration > DICOM > Assisted Rendering**, add rendering policies to specify which DICOM images should be pre-rendered or which SOP instances should be excluded from rendering.

To add a policy for assisted rendering, perform the following steps.

1. Go to **Administration > DICOM > Assisted Rendering**. The **Policies** tab displays existing policies for assisted rendering.
2. Select **Add New**. The Add Assisted Rendering Policy page displays.
3. In the **Policy Attributes** section, complete the following fields:
 - **Policy Name:** Enter a name for the policy.
 - **Excluded SOP Class UIDs from Prerendering:** Select **Edit**. Click in the **Search** field, select one or more SOP classes to exclude, and then select **Close**.
 - **Receiving AEs:** Select **Any Local AE**, or specify the local AE.
 - **Source AEs:** Select **Any Remote AE**, or specify the remote AE.
 - **Decision:** Select whether to prerender.
 - **Enable Prerendering Non-pending Studies:** Select to turn on prerendering for non-pending studies.
 - **Enable Prerendering of Priors:** Select to turn on prerendering of prior studies.
 - **Maximum Number of Priors to Prerender:** Enter a number.
4. In the **Advanced Options** section, complete the following fields:
 - **Request Priority:** Enter a number that designates the priority of the request.
 - **Application Category:** Select an option.
5. Select **Save**. The assisted rendering policy is added, and the **Status** column displays **Disabled**.
6. Turn on the policy you added by selecting **Enable**. The **Status** column displays **Enabled**.

Editing policies for assisted rendering

To edit an existing policy for assisted rendering, perform the following steps.

1. Go to **Administration > DICOM > Assisted Rendering**. The **Policies** tab displays existing policies for assisted rendering.
2. In the row that includes the policy that you want to edit, select **Edit**. The Edit Assisted Rendering Policy page displays.
3. Modify information in any of the fields, and then select **Save**.

Turning off policies for assisted rendering

To turn off a policy for assisted rendering, perform the following steps.

1. Go to **Administration > DICOM > Assisted Rendering**. The **Policies** tab displays existing policies for assisted rendering.
2. In the row that includes the policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Configuring settings for assisted rendering policies

From **Administration > DICOM > Assisted Rendering > Advanced Settings** tab, turn on pre-rendering for specific image types.

To configure settings for assisted rendering policies, perform the following steps.

1. Go to **Administration > DICOM > Assisted Rendering > Advanced Settings** tab.
2. Select **Enable Prerendering** to turn on prerendering.
3. From the **Image Type** dropdown list, select the type of image that can be prerendered.
4. Select **Save**. A message displays confirming the configuration changes are saved.

Deleting policies for assisted rendering

To delete an existing policy for assisted rendering, perform the following steps.

1. Go to **Administration > DICOM > Assisted Rendering**. The **Policies** tab displays existing policies for assisted rendering.
2. In the row that includes the policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The policy is removed.

Routing Policies

From **Administration > DICOM > Routing Policies**, define and maintain policies for routing incoming studies to specific remote AEs.

Adding routing policies

Filter the list of routing policies by entering a term in the **Filter** field.

To add a routing policy, perform the following steps.

1. Go to **Administration > DICOM > Routing Policies**. The **Policies** tab displays.
2. Select **Add New**. The Add Routing Policy page displays the Source AEs page.
3. Select the sources from which studies originate that will trigger the routing policy.
 - In the **Remote AEs** section, select whether to route studies coming from all configured remote AEs or route studies coming from specific remote AEs.
 - In the **Other Sources** section, select additional sources, such as imported from CD media, from which studies may originate.
4. Select **Next**. The Receiving AEs page displays. If you need to return to a previous page, select **Previous**.
5. Select which AEs should receive the data to be routed, and then select **Next**. The Destinations page displays.
6. Select the routing destinations for **Local AEs** and for **Remote AEs**, and then select **Next**. The Masquerading page displays.
7. Turn on masquerading for a remote AE title by selecting the **Masquerading** option next to the remote AE title. The **Masquerading** option only displays when masquerading has been turned on for a remote AE. Select **Next**. The Dataset Triggers page displays.
8. Configure the following dataset triggers as needed:
 - **Match Tags**: Determine which DICOM® data to route by matching tag values. Apply Boolean logic criteria.
 - **Match Assigned Radiologist**: Select the radiologist for which to trigger the routing policy. If configured, the system will route a study only if the radiologist assigned to the corresponding requested procedure matches.
9. Select **Next**. The Active Window page displays.

10. Select whether the routing policy is **Always Active**, or specify the day and time when the routing policy is active. Select **Next**. The Job Creation Options page displays.
11. Configure the following options for scheduling routing jobs:
 - **Job Options**: Select the type of job to be routed, and select whether to create a secondary queue for priority jobs.
 - **Schedule**: Select when routing should begin after the study is received.
12. Select **Next**. The Restructure Study page displays.
13. Modify the study structure, including the **Tag Morphing Policy** and **Value Composition**, prior to sending it to the destination. Studies can be morphed using a predefined anonymization policy or by defining a custom tag morphing policy specific to the rule. When modifications are applied, they are visible at the destination only; the study remains unmodified on the system. Select **Next**. The Tag Morphing page displays.
14. Select a tag morphing option for outbound studies triggered by this routing policy, and then select **Next**. The Notification page displays.
15. For each recipient email address that is listed, select **Success** and **Failures**, and the recipient receives an email notification based on the outcome of the routing job triggered by this policy. Select **Next**. The Advanced Options page displays.
16. Select any of the following options for routing studies:
 - **Preferred Transfer Syntax**: Select the preferred transfer syntax for the routing jobs triggered by this routing policy.
 - **Replication**: Select to replicate the study modifications and the study status changes to the destination AE.
 - **Route Inconsistent Studies**: Select to always route incoming studies that have inconsistent data.
17. Select **Next**. The Description page displays.
18. In the **Description** field, enter a name or a brief description that identifies this routing policy, and then select **Next**. The Review page displays.
19. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
20. Review the configuration, and select **Finish**. The routing policy is added, and the **Status** column displays **Enabled**.

Editing information for routing policies

From **Administration > DICOM > Routing Policies > Policies** tab, edit information for existing routing policies.

Filter the list of routing policies by entering a term in the **Filter** field.

To edit information for a routing policy, perform the following steps.

1. Go to **Administration > DICOM > Routing Policies > Policies** tab.
2. In the row that includes the routing policy that you want to edit, select **Edit**. The Edit Routing Policy page displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. The routing policy changes are saved, and the **Status** column displays **Enabled**.

Turning off routing policies

To turn off a routing policy, perform the following steps.

1. Go to **Administration > DICOM > Routing Policies > Policies** tab.
2. In the row that includes the routing policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Configuring settings for routing policies

From **Administration > DICOM > Routing Policies > Settings** tab, configure settings, such as routing job retries, for all routing policies that are turned on.

To configure the settings for routing policies, perform the following steps.

1. Go to **Administration > DICOM > Routing Policies > Settings** tab.
2. Configure any of the following routing parameters:
 - **Query Frequency**: Enter the number in seconds that the worklist manager will check for new routing jobs.
 - **Keep Completed Jobs**: Enter the maximum number in days that completed jobs will be maintained on the routing worklist before they are deleted.
 - **Maximum Job Retries**: Specify the maximum number of attempts an unsuccessful job will be retried before the job is marked as failed.

- **Allow Concurrent Series-level Jobs:** Select to allow series-level jobs to run concurrently.
 - **Allow Concurrent Image-level Jobs:** Select to allow image-level jobs to run concurrently.
 - **Default Transfer Syntax:** Select the default transfer syntax for routed images. This setting can be overridden by a preferred transfer syntax that is configured in a specific routing policy.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Deleting routing policies

To delete an existing routing policy, perform the following steps.

1. Go to **Administration > DICOM > Routing Policies > Policies** tab.
2. In the row that includes the routing policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The routing policy is removed.

Prefetching Policies

From **Administration > DICOM > Prefetching Policies**, define and maintain policies for retrieving prior patient studies when a prefetching policy is triggered by scheduled exams on the Modality Worklist.

Adding prefetching policies

Filter the list of prefetching policies by entering a term in the **Filter** field.

To add a prefetching policy, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies**. The **Policies** tab displays.
2. Select **Add New**. The Add Prefetching Policy page displays the MWL Servers page.
3. Select one or more Modality Worklist (MWL) servers to query when processing the prefetching rule, and then select **Add**. This option is not available if querying a local server. Select **Next**. The MWL Query Criteria page displays. If you need to return to a previous page, select **Previous**.
4. Select the **Scheduled Station AEs** and **Scheduled Modality** that will be used in the MWL query. Select **Next**. The MWL Results Refinement page displays.
5. Add or remove matching criteria for scheduled exams on the MWL, and then select **Next**. The Patient Identification page displays.
6. Select a patient identification method and any corresponding parameters that will be used to identify the same patient when searching for prior studies. Select **Next**. The Fetching Sources page displays.
7. Select the **Local AEs** and **Remote AEs** from which the priors will be fetched, and then select **Next**. The Fetching Type page displays.
8. Select a method in which priors will be fetched, and then select **Next**. The Prioritize Sources page displays.
9. Designate the order in which to query the fetching sources by selecting a source and then selecting **Move Up** or **Move Down**. Select **Next**. The Prior Criteria page displays.
10. Add or remove matching criteria for prior studies, and then select **Next**. The Prior Refinement page displays.
11. Add or remove matching criteria for prior series, and then select **Next**. The Prior Limit page displays.
12. Select from the following limits for prior studies:
 - **Limit the number of prior studies that will be fetched**, and enter the limit number.
 - **Limit the age of the prior studies that will be fetched**, and enter the study age in months.
13. Select **Next**. The Destinations page displays.
14. Select the **Local AEs** and **Remote AEs** destinations to which to send the priors, and then select **Next**. The Tag Morphing page displays.
15. Select a tag morphing method for outbound priors triggered by this policy.
 - If you select a morphing option, read and understand the risk statement that displays, and select **I understand the risks**.
 - If you select the option to define a custom tag morphing policy, select an existing morph tag or enter a tag. Use the **Regular Expression Test Tool** to verify that the morphing tag functions as expected.
16. Select **Next**. The Scheduling page displays.
17. Configure the following scheduling settings:
 - In the **Query Horizon** field, enter the number of days ahead to check the MWL for scheduled procedures. The default is to query 1 day ahead. Select **Limit** to only load prefetches during business hours.
 - Select **Immediate** to initiate fetching of priors immediately when procedures are available within the query horizon.
 - If you did not select **Immediate**, then in the **Prefetch** field, enter the number in hours before a scheduled procedure to begin fetching prior records.
18. Select **Next**. The Advanced Options page displays.
19. Select any of the following configuring options:
 - **Preferred transfer syntax:** Select a syntax from the dropdown list.
 - **High Priority:** Select to prioritize all jobs triggered by the prefetching rule.

20. Select **Next**. The Description page displays.
21. In the **Description** field, enter a name or a brief description that identifies this prefetching policy, and then select **Next**. The Review page displays.
22. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
23. Review the configuration, and select **Finish**. The routing policy is added, and the **Status** column displays **Enabled**.

Editing information for prefetching policies

From **Administration > DICOM > Prefetching Policies > Policies** tab, edit information for existing prefetching policies.

Filter the list of prefetching policies by entering a term in the **Filter** field.

To edit information for a prefetching policy, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies > Policies** tab.
2. In the row that includes the prefetching policy that you want to edit, select **Edit**. The Edit Prefetching Policy page displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. The prefetching policy changes are saved, and the **Status** column displays **Enabled**.

Turning off prefetching policies

To turn off a prefetching policy, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies > Policies** tab.
2. In the row that includes the prefetching policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**, and the following message displays: To view prefetch jobs, go to the Pre/Post Fetching Worklist page under Transfers.

Configuring settings for prefetching policies

From **Administration > DICOM > Prefetching Policies > Settings** tab, configure the location of the MWL server and the frequency of the query.

The business hours that display on the **Settings** tab are read-only. Settings for business hours are configured in **Administration > System > General Settings**.

To configure the settings for a prefetching policy, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies > Settings** tab.
2. In the **Settings** section, complete the following fields:
 - **Server**: Select whether the location of the modality worklist is **Local** or **Remote**. If you select remote, then select the server. Add or remove servers by selecting the plus or minus icon, respectively.
 - **Query Frequency**: Enter a number in minutes by which to query the MWL server.
3. Select **Save**. The settings are saved, and the following message displays: To view prefetch jobs, go to the Pre/Post Fetching Worklist page under Transfers.

Querying MWL responses

From **Administration > DICOM > Prefetching Policies > Query** tab, view what responses are returned by the MWL server when setting up a prefetching rule or when troubleshooting a particular issue.

To manually query an MWL server, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies > Query** tab.
2. From the **Called AE Title** dropdown list, select the MWL server to query.
3. In the **C-FIND Request Criteria** fields, enter the query criteria. Query for all items by leaving all the fields empty.
4. Select **Query**. The responses that match your query criteria display at the bottom of the tab.
5. Clear the information in the **C-FIND Request Criteria** fields by selecting **Clear**.

Deleting prefetching policies

To delete an existing prefetching policy, perform the following steps.

1. Go to **Administration > DICOM > Prefetching Policies > Policies** tab.
2. In the row that includes the prefetching policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The policy is removed.

Postfetching Policies

From **Administration > DICOM > Postfetching Policies**, define and manage policies for routing prior patient studies to another destination when a postfetching policy is triggered by an incoming study.

Adding postfetching policies

Filter the list of postfetching policies by entering a term in the **Filter** field.

To create a postfetching policy, perform the following steps.

1. Go to **Administration > DICOM > Postfetching Policies**.
2. Select **Add New**. The Add Postfetching Policy page displays the AE Trigger options.
3. Select the **Local and Remote AEs** from which studies originate, and then select which **Local AEs** receive the data. Select **Next**. The Dataset Trigger page displays.
4. Add or remove triggering criteria for postfetching, and then select **Next**. The Patient Identification page displays. If you need to return to a previous page, select **Previous**.
5. Select a method for identifying patients, and select any corresponding parameters that will be used to identify the same patient when searching for studies. Select **Next**. The Fetching Sources page displays.
6. Select the **Local AEs** and **Remote AEs** from which the priors will be fetched, and then select **Next**. The Fetching Type page displays.
7. Select a method by which priors will be fetched, and then select **Next**. The Prioritize Sources page displays.
8. Designate the order in which to query the fetching sources by selecting a source and then selecting **Move Up** or **Move Down**. Select **Next**. The Prior Criteria page displays.
9. Add or remove matching criteria for prior studies, and then select **Next**. The Prior Refinement page displays.
10. Add or remove matching criteria for prior series, and then select **Next**. The Prior Limit page displays.
11. Select from the following limits for prior studies:
 - Limit the number of prior studies that will be fetched, and enter the limit number.
 - Limit the age of the prior studies fetched, and enter the study age in months.
12. Select **Next**. The Destinations page displays.
13. Select the **Local AEs** and **Remote AEs** destinations to which to send the priors, and then select **Next**. The Tag Morphing page displays.
14. Select a method for tag morphing for outbound priors that are triggered by this policy, and then select **Next**. The Scheduler page displays.
15. Select when a postfetching policy should be initiated, and designate the time as required. The Advanced Options page displays.
16. Select the study to be fetched, the action to take, and the preferred transfer syntax. Select **Next**. The Description page displays.
17. In the **Description** field, enter a name or a brief description that identifies this postfetching policy, and then select **Next**. The Review page displays.
18. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
19. Review the configuration, and select **Finish**. The postfetching policy is added, and the **Status** column displays **Enabled**.

Editing information for postfetching policies

From **Administration > DICOM > Postfetching Policies**, edit information for existing postfetching policies.

Filter the list of postfetching policies by entering a term in the **Filter** field.

To edit information for a postfetching policy, perform the following steps.

1. Go to **Administration > DICOM > Postfetching Policies**.
2. In the row that includes the postfetching policy that you want to edit, select **Edit**. The Edit Postfetching Policy page displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. The postfetching policy changes are saved, and the **Status** column displays **Enabled**.

Turning off postfetching policies

To turn off a postfetching policy, perform the following steps.

1. Go to **Administration > DICOM > Postfetching Policies**.
2. In the row that includes the postfetching policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Deleting postfetching policies

To delete an existing postfetching policy, perform the following steps.

1. Go to **Administration > DICOM > Postfetching Policies**.
2. In the row that includes the postfetching policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The postfetching policy is removed.

Tag Morphing Policies

From **Administration > DICOM > Tag Morphing Policies**, define and maintain tag morphing policies, and configure settings for anonymization.

Understanding tag morphing

Tag morphing refers to changing the values in one or more of the DICOM[®] attributes that make up a DICOM tag. Create policy-based tag morphing rules to modify DICOM header information, such as patient demographics and image dimensions, and then automate the DICOM tag changes for externally generated studies.

Examples of DICOM tag modifications include, but are not limited to, the following:

- **Delete:** Remove a tag from the dataset.
- **Empty:** Clear the value of a tag.
- **Replace:** Replace the value of a tag with another value.
- **Copy:** Copy the value of a tag to another tag.
- **Prefix:** Prepend the value of a tag with a prefix.
- **Suffix:** Append a suffix to the value of a tag.
- **Randomize:** Replace the value of a tag with a randomly generated number.
- **Round Date:** Round a date to the closest year or half-year.
- **Anonymize by gender:** Anonymize a patient name based on sex.

Applying tag morphing to studies

Apply tag morphing to studies as they are received inbound or sent outbound.

- **Inbound studies:** When applied inbound, studies are morphed as they are received, prior to storage. After a study is stored, any modifications to it will become visible to the user and other systems via query/retrieve. Inbound tag morphing is currently applicable when importing studies after any QC reconciliation is completed.
- **Outbound studies:** When applied outbound, studies are morphed as they are sent across the wire; any modifications applied are visible at the destination system only. Outbound tag morphing is currently applicable for outbound studies that are triggered by routing, prefetching, and/or postfetching.

Also apply tag morphing to studies statically or dynamically.

- **Static:** Static tag morphing means that the tag modifications are fixed, known ahead of time, and always applied the same way. For example, append site-specific prefixes to patient identifiers, or update the institution name.
- **Dynamic:** With dynamic tag morphing, the tag modifications may vary depending on the context, and the values to apply may not be known until runtime. For example, the values to apply to a prefetched study may be obtained from the scheduled exam on the Modality Worklist, whereas the values to apply to a postfetched study may be obtained from the current study that triggered it. Using dynamic tag morphing, the same study can be morphed in different ways to different destinations. This may be useful for dealing with patient inconsistencies in studies from different sources or when each destination requires a site-specific MRN.

Note that the original DICOM instance files that are stored on the PACS are always intact and unmodified; any modifications applied, no matter how they are applied, are maintained separately by the system. This ensures that the original data are available if needed, regardless of how tag morphing is employed at a particular site.

Adding tag morphing policies

From **Administration > DICOM > Tag Morphing Policies**, add policies for tag morphing.

Filter the list of tag morphing policies by entering a term in the **Filter** field.

To create a tag morphing policy, perform the following steps.

1. Go to **Administration > DICOM > Tag Morphing Policies > Policies** tab.
2. From the **Add New** dropdown list, select one of the following options:
 - Empty Policy: Create a new tag morphing policy.
 - Template - Anonymization Policy: Create an anonymization policy based on a predefined template.
3. From the Edit Tag Morphing Policy page, in the **Policy Name** field, enter a name for the policy.
4. Perform any of the following actions:
 - Select a **DICOM Tag** from the dropdown list.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a tag morphing policy by selecting the plus or minus icon, respectively.
5. Select **OK**. A message displays confirming the anonymization policy is saved.

Editing information for tag morphing policies

From **Administration > DICOM > Tag Morphing Policies > Policies** tab, edit information for existing tag morphing policies.

Filter the list of tag morphing policies by entering a term in the **Filter** field.

To edit information for a tag morphing policy, perform the following steps.

1. Go to **Administration > DICOM > Tag Morphing Policies > Policies** tab.
2. In the row that includes the tag morphing policy that you want to edit, select **Edit**. The Edit Tag Morphing Policy page displays.
3. Perform any of the following actions:
 - Select a **DICOM Tag** from the dropdown list.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a tag morphing policy by selecting the plus or minus icon, respectively.
4. Select **OK**. A message displays confirming the anonymization policy is saved.

Configuring anonymization settings for tag morphing policies

To configure the anonymization settings for all tag morphing policies, perform the following steps.

1. Go to **Administration > DICOM > Tag Morphing Policies > Anonymization Settings** tab.
2. In the **Anonymization Mapping** section, select **Enable** for the system to maintain a list of patients and their corresponding anonymized IDs and names.
3. In the **Anonymized Patient IDs** section, in the **Patient ID Prefix** field, enter a prefix that will be automatically added to a patient ID that is being anonymized using a UUID or sequential number.
4. In the **Anonymized Patient Names** section, enter the default names to use when anonymizing patient names based on sex.
5. Select **Save**. A message displays confirming the policy is saved.

Deleting tag morphing policies

To delete an existing tag morphing policy, perform the following steps.

1. Go to **Administration > DICOM > Tag Morphing Policies > Policies** tab.
2. In the row that includes the tag morphing policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. A message displays confirming the policy is removed.

DICOM Mapping Policy

From **Administration > DICOM > DICOM Mapping Policy**, define inbound and outbound DICOM[®] mapping policies.

Turning on outbound DICOM mapping policies

Outbound DICOM mappings are applied whenever instances of the specified modality type are sent to the selected AEs. The original data stored on the source AE will not be modified.

To turn on outbound DICOM mapping policies, perform the following steps.

1. Go to **Administration > DICOM > DICOM Mapping Policy**. The **Outbound** tab displays.
2. Select **Enable**. The mapping parameters display.
3. Perform any of the following actions:
 - Select an **AE Title** from the dropdown list.
 - Select a **Modality** from the dropdown list
 - Select a **DICOM Tag** from the dropdown list.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a DICOM mapping policy by selecting the plus or minus icon, respectively.
4. Select **Save**. The outbound mapping policy is turned on, and a message displays confirming the configuration changes are saved.

Turning on inbound DICOM mapping policies

Inbound DICOM mappings are applied whenever studies are received from the selected remote AEs. All instances of the study will be modified based on the policy and stored as is.

To turn on inbound DICOM mapping policies, perform the following steps.

1. Go to **Administration > DICOM > DICOM Mapping Policy > Inbound** tab.
2. Select **Enable**. The mapping parameters display.
3. Perform any of the following actions:
 - Select an **AE Title** from the dropdown list.
 - Select a **DICOM Tag** from the dropdown list.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a DICOM mapping policy by selecting the plus or minus icon, respectively.
4. Select **Save**. The inbound mapping policy is turned on, and a message displays confirming the configuration changes are saved.

Resetting inbound and outbound DICOM mapping policies

To reset inbound and outbound DICOM mapping policies, perform the following steps.

1. Go to **Administration > DICOM > DICOM Mapping Policy**, and select the **Inbound** tab or **Outbound** tab.
2. Select **Reset**. The Reset DICOM Mapping Policy dialog displays.
3. Confirm the reset, and then select **Yes**. All mapping policies are removed, and the respective **Enable** policy option is cleared.

Availability Notification Policies

From **Administration > DICOM > Availability Notification Policies**, define and maintain policies for availability notifications.

Adding policies for availability notifications

Filter the list of availability notification policies by entering a term in the **Filter** field.

To add a policy for an availability notification, perform the following steps.

1. Go to **Administration > DICOM > Availability Notification Policies**.
2. Select **Add New**. The Instance Availability Notification - Source AEs page displays.
3. Select the remote AEs from which the studies originate, and then select **Next**. The Instance Availability Notification - Receiving AEs page displays. If you need to return to a previous page, select **Previous**.
4. Select which local AEs receive the studies considered for notification, and then select **Next**. The Instance Availability Notification - Notification Recipients page displays.
5. Select the remote AEs that are the recipients of the availability notifications, and then select **Next**. The Instance Availability Notification - Description page displays.
6. In the **Description** field, enter a name or a brief description that identifies this notification, and then select **Next**. The Instance Availability Notification - Summary page displays.
7. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Instance Availability Notification - Summary page

displays.

8. Review the configuration, and select **Finish**. The availability notification notification policy is added, and the **Status** column displays **Enabled**.

Editing information for availability notification policies

From **Administration > DICOM > Availability Notification Policies**, edit information for existing availability notification policies.

Filter the list of availability notification policies by entering a term in the **Filter** field.

To edit information for an availability notification policy, perform the following steps.

1. Go to **Administration > DICOM > Availability Notification Policies**.
2. In the row that includes the availability notification policy that you want to edit, select **Edit**. The Instance Availability Notification - Source AEs page displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Instance Availability Notification - Summary page displays.
4. Review the configuration, and select **Finish**. The availability notification policy changes are saved, and the **Status** column displays **Enabled**.

Turning off policies for availability notifications

To turn off an availability notification policy, perform the following steps.

1. Go to **Administration > DICOM > Availability Notification Policies**.
2. In the row that includes the availability notification policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Deleting policies for availability notifications

To delete an existing availability notification policy, perform the following steps.

1. Go to **Administration > DICOM > Availability Notification Policies**.
2. In the row that includes the availability notification policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The policy is removed.

Teaching File Policy

The system maintains a default teaching file policy that conforms to the de-identification requirements in the DICOM[®] attribute confidentiality profiles. From **Administration > DICOM > Teaching File Policy**, change this default teaching file policy to meet site-specific needs.

Create anonymization rules for a specific patient study record from **Studies > Study Search**. Patient study records that have been anonymized display from **Studies > Teaching File**.

Changing default teaching file policy

Consider the following when changing the default teaching file policy.

- All the unique identifiers (UIDs) are internally processed by the anonymization function. New UID's will be automatically assigned to each dataset. It is not necessary to define any policy for UID attributes.
- Only one action is allowed to be defined for one attribute.
- The actions Round Date To Year and Round Date To Half Year can only be applied to DICOM attributes with VR type DA.
- Be cautious when applying delete and empty actions to an attribute.
 - DICOM type 1 attributes should never be deleted or emptied.
 - DICOM type 2 attributes should never be deleted, but can be emptied.

To change the default teaching file policy, perform the following steps.

1. Go to **Administration > DICOM > Teaching File Policy**. The attributes applied to the default teaching file policy display.
2. Delete an attribute from the policy by selecting the minus icon for that attribute.

3. Add an attribute to the policy by selecting the plus sign in an attribute row and then selecting one of the following actions for the attribute.
 - **Delete:** Delete the attribute from the dataset.
 - **Empty:** Set the attribute to blank, but still keep this attribute in dataset.
 - **Replace:** Replace the attribute value with a user-provided string.
 - **Prefix:** Prefix the attribute value with a user-provided string.
 - **Suffix:** Suffix the attribute value with a user-provided string.
 - **Randomize:** Assign a random value to the attribute.
 - **Randomize With Prefix:** Assign a random value with a user-provided prefix to the attribute.
 - **Randomize With Suffix:** Assign a random value with a user-provided suffix to the attribute.
 - **Round Date To Year:** Round a date attribute to year. For example, 19800401 will be rounded to 19800101; 19800828 will be rounded to 19810101.
 - **Round Date To Half Year:** Round a date attribute to half year. For example, 19800401 will be rounded to 19800101; 19800828 will be rounded to 19800701.
4. Complete the value field, as applicable.
5. Select **Save**. A message displays confirming the configuration changes are saved.

Resetting teaching file policy

To reset a teaching file policy to the default values, perform the following steps.

1. Go to **Administration > DICOM > Teaching File Policy**. The attributes applied to the default teaching file policy display.
2. Select **Reset**. The Reset Teaching File Policy dialog displays.
3. Confirm the reset, and then select **Yes**. The teaching file policy is reset to the default teaching file policy.
4. Select **Save**. A message displays confirming the configuration changes are saved.

Import Service

From **Administration > DICOM > Import Service**, define and maintain import service policies.

Because studies imported into the PACS appliance may be subject to the quality control process at a specific site, the studies require user intervention to reconcile any patient inconsistencies in the data prior to storage. Configure how the system deals with imported studies and whether tag morphing should be applied to those studies after the QC process.

Adding import service policies

Tag morphing can be applied to imported studies after user reconciliation, but prior to storage. Tag morphing may also be applied to studies from all import sources or from a specific import source only.

To add an import (tag morphing) service policy, perform the following steps.

1. Go to **Administration > DICOM > Import Service**. The **Policies** tab displays existing import service policies.
2. Select **Add New**. The Edit Import Service Policy page displays.
3. In the **Policy Name** field, enter a name for the policy.
4. Perform any of the following actions:
 - Select the **Import Source** from the dropdown list.
 - Select a **DICOM Tag**.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a tag morphing policy by selecting the plus or minus icon, respectively.
5. Select **OK**. A message displays confirming the import service policy is saved.

Editing information for import service policies

To edit information for an import service policy, perform the following steps.

1. Go to **Administration > DICOM > Import Service > Policies** tab.
2. In the row that includes the import service policy that you want to edit, select **Edit**. The Edit Import Service Policy page displays.
3. Perform any of the following actions:
 - Modify the **Policy Name**.
 - Change the **Import Source** from the dropdown list.
 - Change a **DICOM Tag**.
 - Select an **Action** for the tag.
 - Enter a **Parameter value** for the action, as appropriate.
 - Add or remove a tag morphing policy by selecting the plus or minus icon, respectively.

4. Select **OK**. A message displays confirming the import service policy is saved.

Configuring settings for reconciling imported studies

Prefetching policies must be created in **Administration > DICOM > Prefetching Policies** before they can be applied to imported studies.

To configure settings for reconciling imported studies, perform the following steps.

1. Go to **Administration > DICOM > Import Service > Settings** tab.
2. In the **Import Reconciliation Settings** section, complete the following fields:
 - **Reconciliation AE Alias**: Enter the AE alias for importing studies via DICOM C-STORE.
 - **Priors Exchange Prefetching Policy**: Select a prefetching policy that will find imported priors and send them to the priors exchange peer.
 - **Bypass Reconciliation Criteria**: Select the criteria for bypassing the Reconciliation Worklist.
3. Select **Save**. A message displays confirming the import service policy configuration is saved.

Configuring settings for storing reconciled studies

Tag morphing policies must be created in **Administration > DICOM > Tag Morphing Policies** before they can be applied to reconciled studies.

To configure settings for storing reconciled studies, perform the following steps.

1. Go to **Administration > DICOM > Import Service > Settings** tab.
2. In the **Import Store Settings** section, complete the following fields:
 - **Import Destination**: Select the default destination for reconciled studies.
 - **Tag Morphing Policy**: Select the tag morphing policy to apply to imported studies after QC.
3. Select **Save**. A message displays confirming the import service policy configuration is saved.

Configuring settings for retaining studies in worklists

To configure settings for retaining studies in worklists, perform the following steps.

1. Go to **Administration > DICOM > Import Service > Settings** tab.
2. In the **Worklist Management** section, complete the following fields:
 - **Retention Period Enable**: Select to turn on study retention.
 - Enter a number, and then select the amount of time studies on the Reconciliation Worklist and Import Store Worklist are retained. Any studies older than the specified retention period will be deleted automatically.
3. Select **Save**. A message displays confirming the import service policy configuration is saved.

Deleting import service policies

To delete an existing import service policy, perform the following steps.

1. Go to **Administration > DICOM > Import Service > Policies** tab.
2. In the row that includes the import service policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion by selecting **Yes**. The policy is removed.

Study Status

From **Administration > DICOM > Study Status**, specify the default study status for all studies that are received.

Configuring study status

Study status is not a DICOM[®] Standard attribute and may not be compatible with some appliances. Specifically, the Accept from Remote AE option only works with compatible systems.

To specify the default study status for incoming studies, perform the following steps.

1. Go to **Administration > DICOM > Study Status**.
2. Complete the following fields:
 - **Hold Period**: Enter the number of days to hold a study.
 - **Priors Cutoff Period**: Enter the number of days for prior cutoff.

- **Default Study Status:** Select the default study status to apply to all pre/post fetched studies.
- 3. In the **Non-Pre/Post Fetched Studies** section, for each **Remote AE Title** listed, select a **Viewer Study Status**.
- 4. Select **Save**. A message displays confirming the configuration is saved.

Transparent Proxy

From **Administration > DICOM > Transparent Proxy**, define and maintain transparent proxies.

A transparent proxy is an alias for a group of application entities (AEs) that other DICOM-compliant devices can communicate with as a single AE. When query or retrieve requests are received, the proxy will forward them to all of its target AEs, collate the results, and then send the appropriate responses to the original requester. For retrieve requests, the proxy will first pull the requested data to a designated local proxy AE, and then push the requested data to the destination AE.

Adding transparent proxies

Filter the list of transparent proxies by entering a term in the **Filter** field.

Only registered remote AEs with write permission to the proxy AE are eligible to become proxy targets because the proxy may need to pull data from the target.

To add a transparent proxy, perform the following steps.

1. Go to **Administration > DICOM > Transparent Proxy**. The list of existing transparent proxies displays.
2. Select **Add New**. The Transparent Proxy - Configuration page displays.
3. Complete the following fields:
 - **Proxy:** Enter a name for the transparent proxy.
 - **Description:** Enter a brief description of the transparent proxy.
 - **Local AE:** Select the local AE to cache retrieved DICOM objects.
4. Select **Next**. The Transparent Proxy - Proxy Targets page displays. If you need to return to a previous page, select **Previous**.
5. Select the **Local AEs** and **Remote AEs** that are the targets for the proxy, and then select **Next**. The Transparent Proxy - Duplicate Policy page displays.
6. Designate the order in which targets are prioritized by selecting a target and then selecting **Move Up** or **Move Down**. If duplicate data are found on multiple targets, then the result from the highest-ranking target will be used when preparing the proxy responses. Select **Next**. The Transparent Proxy - Permissions page displays.
7. Select the registered remote AEs that have permission to access the proxy, and then select **Next**. The Transparent Proxy - Summary page displays.
8. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Summary page displays.
9. Review the configuration, and select **Finish**. The transparent proxy is added, and a message displays confirming the configuration changes are saved.

Editing information for transparent proxies

From **Administration > DICOM > Transparent Proxy**, edit information for existing transparent proxies.

Filter the list of transparent proxies by entering a term in the **Filter** field.

To edit transparent proxy information, perform the following steps.

1. Go to **Administration > DICOM > Transparent Proxy**.
2. In the row that includes the transparent proxy that you want to edit, select **Edit**. The Transparent Proxy - Configuration page displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Summary page displays.
4. Review the configuration, and select **Finish**. A message displays confirming the configuration changes are saved.

Deleting transparent proxies

From **Administration > DICOM > Transparent Proxy**, delete transparent proxies.

Filter the list of transparent proxies by entering a term in the **Filter** field.

To delete a transparent proxy, perform the following steps.

1. Go to **Administration > DICOM > Transparent Proxy**.

2. In the row that includes the transparent proxy that you want to delete, select **Delete**. The Delete Transparent Proxy dialog displays.
3. Confirm the deletion by selecting **Yes**. A message displays confirming that the transparent proxy is removed.

RT Service

From **Administration > DICOM > RT Service**, configure the RT Service to create radiation therapy (RT) cases that will display in the radiology worklist of the corresponding RT viewer application.

Configuring RT Service

Examples of objects that are received and used to create RT cases may include, but are not limited to, the following:

- Portal images are low resolution, single-frame CTs that aid users in pointing a scanner. Generally, portal images are 2D and 3D cases that may be used for pre-treatment patient positioning reviews.
- Cone beam CTs (CBCT) are valid treatment structure sets that point to a CBCT.

To configure the RT Service, perform the following steps.

1. Go to **Administration > DICOM > RT Service**.
2. Select all of the following options:
 - **Create Portal Image Worklist Entry**
 - **Create CBCT Worklist Entry**
 - **Create Dose Worklist Entry**
 - **Create CR Worklist Entry**
 - **Create REG Worklist Entry**
 - **Auto Route RT Review Report**
3. Select **Save**. A message displays confirming the configuration changes are saved.

HL7

HL7 is a set of standards recognized by the American National Standards Institute (ANSI) that provides guidelines for the exchange, allocation, and retrieval of patient medical information. HL7 may also be used to provide an automated interface for placing orders onto the modality workload from your current EMR/RIS system.

You must have a license to use the HL7 functionality. Contact your sales representative if you want to purchase an HL7 license for your PACS system.

To ensure full compatibility with your site workflows, the format of all HL7 messages to be exchanged should have been reviewed during an earlier HL7 integration. Contact your sales representative to start a new integration or to inquire about adding a new feature not previously discussed.

From **Administration > HL7**, access the following modules:

- **HL7 Service** - Configure settings for the HL7 Service and worklists.
- **HL7 Peers** - Define and maintain HL7 peers.
- **HL7 Stations** - Define and maintain HL7 stations.
- **HL7 Mappings** - Map database entries to HL7 message fields.
- **HL7 Test Tool** - Validate whether mappings parse and display the messages as desired.

HL7 Service

From **Administration > HL7 > HL7 Service**, configure settings for the HL7 Service and HL7 Worklist.

Configuring connection settings for HL7 Service

To configure connection settings for the HL7 Service, perform the following steps.

1. Go to **Administration > HL7 > HL7 Service**. The **Configuration** tab displays.
2. In the **Connection Settings** section, complete the following fields:
 - **Listening Port**: Enter the listening port.
 - **Alternate Listening Port**: Select to turn on an alternate port, and then enter the port number.
 - **Secure Listening Port**: Enter the local port number used for secure transfer.
 - **Secure Transfer Certificate**: Select a certificate that was added from **Administration > System > Certificates > Peer Certificates** category.
 - **Inbound Connection Timeout**: Select **None**, or enter the number in seconds before an idle inbound HL7 connection is released.
 - **Outbound Connection Timeout**: Select **None**, or enter the number in seconds before an idle outbound HL7 connection is released.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring settings for inbound messages for HL7 Service

To configure settings for inbound messages for the HL7 Service, perform the following steps.

1. Go to **Administration > HL7 > HL7 Service**. The **Configuration** tab displays.
2. In the **Inbound Messages** section, in **Inbound Order Policy**, select any of the following options:
 - **Automatically Schedule New Orders**: New orders received will be automatically scheduled on the modality workload; otherwise, they will need to be scheduled from the RIS.
 - **Delete Canceled Orders**: The records for canceled orders will be permanently deleted from the system.
 - **Require New Orders Before Status Updates**: New orders must be received before any status updates can be accepted.
3. From the **Inbound Report Policy** dropdown list, select the method by which inbound reports are imported into the system.
4. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring settings for outbound messages for HL7 Service

To configure settings for outbound messages for the HL7 Service, perform the following steps.

1. Go to **Administration > HL7 > HL7 Service**. The **Configuration** tab displays.
2. In the **Outbound Messages** section, complete the following fields:
 - **Outbound Report Format**: Select the data format for outbound final report messages.

- **Outbound URL Notification Format:** Select the method by which viewer study URLs are embedded within HL7 messages.
 - **Include Study Instance UID:** Select whether to include a custom data segment with the study instance UID corresponding to the report.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring settings for HL7 Service Worklist

To configure settings for the HL7 Service Worklist, perform the following steps.

1. Go to **Administration > HL7 > HL7 Service > Worklist** tab.
2. In the **Batch Export Settings** section, complete the following fields:
 - **Sending Application:** Enter the sending application when exporting one or more messages as a single batch message.
 - **Sending Facility:** Enter the sending facility when exporting one or more messages as a single batch message.
 - **Receiving Application:** Enter the receiving application when exporting one or more messages as a single batch message.
 - **Receiving Facility:** Enter the receiving facility when exporting one or more messages as a single batch message.
3. In the **Worklist Management** section, complete the following fields:
 - **Keep Completed Jobs:** Enter the number in days how long completed jobs are maintained on the HL7 Worklist before they are deleted.
 - **Maximum Job Retries:** Enter the maximum number of retries before the HL7 Service stops trying to send a failed message.
 - **Delete Failed Jobs:** Select to delete failed jobs from the HL7 Worklist. This is turned off by default, so failed jobs will remain indefinitely.
4. Select **Save**. A message displays confirming the configuration changes are saved.

HL7 Peers

From **Administration > HL7 > HL7 Peers**, define and maintain HL7 peers.

The HL7 Service accepts inbound messages only from registered HL7 peers; network connections from unrecognized peers will be automatically rejected.

Adding HL7 peers

To add an HL7 peer, perform the following steps.

1. Go to **Administration > HL7 > HL7 Peers**. The list of existing HL7 peers displays.
2. Select **Add New**. The HL7 Peer - Configuration dialog displays.
3. Complete the following fields:
 - **Name:** Enter a name for the peer.
 - **Host Address:** Enter a valid host address for the peer.
 - **Mapping:** Select a mapping.
4. Select **Next**. The HL7 Peer - Inbound Policy dialog displays. If you need to return to a previous page, select **Previous**.
5. Select the corresponding local AE title, default HL7 station for inbound orders received from the peer, and any message types that should be ignored. Select **Next**. The HL7 Peer - Patient Identification dialog displays.
6. Select a method for identifying patients, and then select **Next**. The HL7 Peer - Outbound Setting dialog displays.
7. Enter the listening port of the peer, and configure additional settings as needed. Select **Next**. The HL7 Peer - Message Triggers dialog displays.
8. Select the appropriate events that will trigger the system to send an outbound HL7 message to the peer, and then select **Next**. The HL7 Peer - Additional Options dialog displays.
9. Select the facilities and assigned radiologists for which the outbound message triggers are turned on, and then select **Next**. The HL7 Peer - Summary dialog displays.
10. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Summary dialog displays.
11. Review the configuration, and select **Finish**. A message displays confirming the HL7 peer was added, and the **Status** column displays **Enabled**.

Editing information for HL7 peers

From **Administration > HL7 > HL7 Peers**, edit information for HL7 peers.

To edit HL7 peer information, perform the following steps.

1. Go to **Administration > HL7 > HL7 Peers**.

2. In the row that includes the HL7 peer that you want to edit, select **Edit**. The HL7 Peer - Configuration dialog displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Summary** in the left pane. The Summary dialog displays.
4. Review the configuration, and select **Finish**. The HL7 peer changes are saved, and the **Status** column displays **Enabled**.

Turning off HL7 peers

When a peer is turned off, it is ignored by the server. Outbound messages that are triggered to the unavailable peer will continue to be spooled to the HL7 Worklist, but will not be sent.

To turn off an HL7 peer, perform the following steps.

1. Go to **Administration > HL7 > HL7 Peers**.
2. In the row that includes the HL7 peer that you want to turn off, select **Disable**. The **Status** column displays **Disabled**, and a message displays confirming the HL7 peer is disabled.
3. To turn on a disabled HL7 peer, select **Enable**. The **Status** column displays **Enabled**, and a message displays confirming the HL7 peer is enabled.

Deleting HL7 peers

To delete an HL7 peer, perform the following steps.

1. Go to **Administration > HL7 > HL7 Peers**.
2. In the row that includes the HL7 peer that you want to delete, select **Delete**. The Delete HL7 Peer dialog displays.
3. Confirm the deletion by selecting **Yes**. The HL7 peer is removed.

HL7 Stations

From **Administration > HL7 > HL7 Stations**, define and maintain HL7 stations.

HL7 stations are used to filter orders by application entity and/or modality type. Configuring HL7 stations may be useful when sites have multiple types of modalities because you can query the modality worklist for only the relevant set of exams.

Adding HL7 stations

From **Administration > HL7 > HL7 Stations**, add HL7 stations.

Naming HL7 stations should be discussed during the HL7 integration process to ensure full compatibility.

To add an HL7 station, perform the following steps.

1. Go to **Administration > HL7 > HL7 Stations**. Existing HL7 stations display.
2. Select **Add New**. The Add New HL7 Station dialog displays.
3. Complete the following fields:
 - **Resource Name**: Enter the name of the resource. This name is used when parsing HL7 messages to filter orders.
 - **Location**: Enter the location of the HL7 station.
 - **Modality**: Select the modality.
 - **Scheduled Station AE**: Select the scheduled station AE.
4. Select **OK**. A message displays confirming the HL7 station is saved.

Editing information for HL7 stations

From **Administration > HL7 > HL7 Stations**, edit information for HL7 stations.

To edit information for HL7 stations, perform the following steps.

1. Go to **Administration > HL7 > HL7 Stations**. Existing HL7 stations display.
2. In the row that includes the HL7 station that you want to edit, select **Edit**. The Edit HL7 Station dialog displays.
3. Modify information in any of the fields, and then select **OK**. A message displays confirming the HL7 station is saved.

Deleting HL7 stations

From **Administration > HL7 > HL7 Stations**, delete HL7 stations.

To delete an HL7 station, perform the following steps.

1. Go to **Administration > HL7 > HL7 Stations**. Existing HL7 stations display.
2. In the row that includes the HL7 station that you want to delete, select **Delete**. The Delete HL7 Station dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the HL7 station is deleted.

HL7 Mappings

From **Administration > HL7 > HL7 Mappings**, map database entries to HL7 message fields. Each HL7 peer in the system has an associated mapping.

Although a mapping may be shared among multiple peers, this practice is not recommended because a change to one mapping, as requested by one peer, also affects other peers that use that mapping.

Adding HL7 mappings

From **Administration > HL7 > HL7 Mappings**, add HL7 mappings.

Adding an HL7 mapping is the process of creating a new mapping based on any existing mappings, such as the following:

- Base Mapping is the *factory* mapping.
- Default Data Mapping

To add an HL7 mapping, perform the following steps.

1. Go to **Administration > HL7 > HL7 Mappings**. Existing HL7 mappings display.
2. Select **Add New**. The Add New HL7 Mapping dialog displays.
3. Complete the following fields:
 - **Alias**: Enter an name for the mapping.
 - **Description**: Enter a brief name or description that identifies the mapping.
 - **Based On**: Select whether you want the mapping to be based on existing base mappings or on the default (hard-coded) data mapping, which is editable.
4. Select **OK**. A message displays confirming the HL7 mapping was added.

Editing HL7 mappings

From **Administration > HL7 > HL7 Mappings**, edit HL7 mappings.

To edit existing HL7 mappings, perform the following steps.

1. Go to **Administration > HL7 > HL7 Mappings**. Existing HL7 mappings display.
2. In the row that includes the HL7 mapping that you want to edit, select **Edit**. The Edit HL7 Mappings page displays.
3. Make changes, and then select **OK**. A message displays confirming the HL7 mapping was saved.

Exporting HL7 mappings

To export HL7 mappings, perform the following step.

Go to **Administration > HL7 > HL7 Mappings**, and then select **Export**. The HL7 mapping file is downloaded to your computer.

Replacing existing HL7 mappings by importing mappings

Importing mappings is useful when you want to copy mappings from one PACS appliance to another PACS appliance.

Only import a mapping file to a PACS appliance that you exported from a PACS appliance. The mapping file name uses the following format: <serialnumber>_<version>.hl7map.

To import HL7 mappings, perform the following steps.

1. Go to **Administration > HL7 > HL7 Mappings**, and then select **Import**. The Import HL7 Mappings dialog displays.
2. Confirm you want to replace existing mappings, and then select **Yes**.
3. Select **Choose File**, select the file, and then select **Open**.
4. Select **Import**. The mapping file is imported and displays in the list.

Deleting HL7 mappings

From **Administration > HL7 > HL7 Mappings**, delete HL7 mappings.

To delete an HL7 mapping, perform the following steps.

1. Go to **Administration > HL7 > HL7 Mappings**. Existing HL7 mappings display.
2. In the row that includes the HL7 mapping that you want to delete, select **Delete**. The Delete HL7 Mapping dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the HL7 mapping is deleted.

HL7 Test Tool

From **Administration > HL7 > HL7 Test Tool**, validate whether mappings parse and display messages as desired. It is recommended to validate a mapping before assigning it to a peer.

For example, when viewing the HL7 Worklist, errors may display in the outbound messages. Select the magnifying glass icon in the row of the error, and the message displays in the HL7 Test Tool. After you select **Parse**, the HL7 Test Tool parses the HL7 message using the mapping that you select in the tool. From the test tool, select a different mapping and see how parsing the message changes from where the system takes values.

Validating HL7 parsing messages

From **Administration > HL7 > HL7 Test Tool > Parse** tab, validate whether a mapping parses a message as expected.

To validate an HL7 parsing message, perform the following steps.

1. Go to **Administration > HL7 > HL7 Test Tool**. The **Parse** tab displays.
2. From the **Mapping** dropdown list, select the mapping that you want to apply, and then select **Parse**. The results display in the text box.
3. Clear the information in the fields by selecting **Clear**.

Composing and testing HL7 messages

From **Administration > HL7 > HL7 Test Tool > Compose** tab, validate whether a mapping displays a message as expected.

To compose and test an HL7 parsing message, perform the following steps.

1. Go to **Administration > HL7 > HL7 Test Tool > Compose** tab.
2. From the **Mapping** dropdown list, select the mapping for which you want to test messages.
3. Select **Compose**.
4. Clear the information in the fields by selecting **Clear**.

Patient

From **Administration > Patient**, access the following modules:

- **Quality Control** - Configure parameters to enhance detection of potential inconsistencies among data in patient records.
- **Identification Domain** - Define and maintain domains for patient identification.
- **Demographics Supplier** - Configure a remote patient demographics supplier.
- **PIX Settings** - Turn on queries for patient identifier cross-referencing (PIX) managers, and configure the PIX manager.

Quality Control

From **Administration > Patient > Quality Control**, configure parameters to enhance detection of potential inconsistencies among data in patient records stored on the PACS.

Configuring parameters for detecting conflicts in patient data

From **Administration > Patient > Quality Control > Conflict Control** tab, change the parameters for detecting conflicts in patient data.

For example, conflicts in patient data may be reported when two or more different persons with the same patient ID are detected within the local system. All the local patient records that are determined to have conflicts in the data are listed in **Patients > Conflict**.

To configure parameters for detecting conflicts in patient data, perform the following steps.

1. Go to **Administration > Patient > Quality Control > Conflict Control** tab.
2. In **Conflict Evaluation Policy**, select the patient demographic data, such as **Name**, **Birth Date**, or **Sex**, that will be considered during conflict evaluation.
3. In **String Matching Policy**, designate the matching parameters to be used when evaluating the patient demographic data.
4. Select **Save**. A message displays confirming the configuration changes are saved.

Configuring data sources for import reconciliation

From **Administration > Patient > Quality Control > Reconciliation Control** tab, configure data sources for import reconciliation.

Patient data that is imported into the PACS appliance can come from different sources, such as the local system, an RIS or PACS provider that supports the MWL Information Data Model, or a system that supports the Remote Patient Root Information Data Model.

Reconciling patient data is an optional step during the import process.

To configure data sources for import reconciliation, perform the following steps.

1. Go to **Administration > Patient > Quality Control > Reconciliation Control** tab.
2. Complete the following fields:
 - **Data Source Type**: Select the type of patient identity repository and search mechanism to use during import reconciliation. The data source type that you select determines whether you need to complete the following fields.
 - **Data Source Name**: Select an AE title to use as the patient identify repository for a remote or MWL data source.
 - **MWL Data Source Policy**: Select whether to query the MWL data source for all exams.
3. Select **Save**. A message displays confirming the configuration is saved.

Assigning score weights to patient demographic data

From **Administration > Patient > Quality Control > Reconciliation Control** tab, assign score weights to the patient demographic data to be used during patient similarity evaluations. The total of the percentages must be 100 percent.

During the patient information reconciliation process, similar patients are detected using a scoring-based algorithm. The configured weights assigned to each patient demographic factor, such as patient ID and sex, will be taken by this algorithm to calculate the similarity score. Candidate patients with a score higher than the specified threshold will be suggested to the user to assist in determining whether the same patient already exists on the specified data source.

To assign score weights to patient demographic data, perform the following steps.

1. Go to **Administration > Patient > Quality Control > Reconciliation Control** tab.
2. In the **Candidate Score Weight** section, enter a percent value for each of the following options. The total of the percentages must be 100 percent. Enter zero (0) if you do not want the factor to be considered during the evaluation.
 - **Patient ID**
 - **First Name**
 - **Last Name**
 - **Middle Name**
 - **Birth Date**
 - **Sex**
3. Select **Save**. A message displays confirming the configuration is saved.

Turning on MWL data correction

From **Administration > Patient > Quality Control > MWL Data Correction** tab, turn on Modality Worklist (MWL) data correction.

If the PACS appliance RIS is used to provide the Modality Worklist, after the modalities send the studies to the PACS, patient information from the inbound studies can be matched against the RIS patient data. If discrepancies exist, then the study can be automatically corrected to use the patient data from RIS.

Data correction of an inbound study is a delayed post-processing service that starts one time daily. After you turn on MWL data correction, you must also schedule a valid time and day on which the service will perform the MWL data correction.

To turn on MWL data correction, complete the following fields.

1. Go to **Administration > Patient > Quality Control > MWL Data Correction** tab.
2. Select **Enable** to turn on MWL data correction.
3. In the **Scheduled Time** dropdown lists, designate the hour and minute that data correction will occur.
4. In the **Scheduled Date** options, select the day or days on which data correction should occur.
5. Select **Save**. A message displays confirming the configuration is saved.

Identification Domain

From **Administration > Patient > Identification Domain**, define and maintain domains for patient identification.

Different data sources may contain different patient data for the same patient. A patient identification domain is an environment in which all the systems and applications consistently use patient data from a single patient source. The PACS system may need to communicate with other systems and applications across patient identification domains to exchange data.

The patient identification domains defined here can be referenced by DICOM[®] Standard remote AEs to indicate different patient sources adopted by different AEs. Multiple AEs can belong to the same domain. The domains also can be used by patient demographics suppliers and for patient identifier cross-referencing (PIX).

Adding domains for patient identification

From **Administration > Patient > Identification Domain > Domains** tab, add domains for patient identification.

To add a domain for patient identification, perform the following steps.

1. Go to **Administration > Patient > Identification Domain**. The **Domains** tab displays.
2. Select **Add New**. The Add New Patient Identification Domain dialog displays.
3. Complete the following fields:
 - **Alias**: Enter an alias for the namespace.
 - **Namespace ID**: Enter a valid ID for the namespace.
 - **Universal ID**: Enter a valid universal ID for the namespace.
4. Select **OK**. A message displays confirming the domain is saved.

Editing information for patient identification domains

To edit information for a patient identification domain, perform the following steps.

1. Go to **Administration > Patient > Identification Domain**. The **Domains** tab displays.

2. In the row that includes the domain that you want to edit, select **Edit**. The Edit Patient Identification Domain dialog displays.
3. Modify information, and then select **OK**. A message displays confirming the domain is saved.

Configuring patient identification domains for local systems

From **Administration > Patient > Identification Domain > Settings** tab, configure the patient identification domain.

The patient identification domain for this PACS appliance system has to be defined for the Patient Demographics Supplier and Patient Identifier Cross-Referencing (PIX) applications to function correctly.

To configure the patient identification domain for this PACS appliance system, perform the following steps.

1. Go to **Administration > Patient > Identification Domain > Settings** tab.
2. In the **Local System Patient Identification Domain** dropdown list, select the local domain, and then select **Save**. A message displays confirming the configuration is saved.

Deleting patient identification domains

You cannot delete a patient identification domain that is referenced by the local system.

To delete a patient identification domain, perform the following steps.

1. Go to **Administration > Patient > Identification Domain**. The **Domains** tab displays.
2. In the row that includes the domain that you want to delete, select **Delete**. The Delete Patient Identification Domain dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the domain is deleted.

Demographics Supplier

From **Administration > Patient > Demographics Supplier**, configure a remote patient demographics supplier.

Patient Demographics Supplier is an HL7 service that provides patient query function through the standard HL7 QBP message. The PACS appliance can act as a client to query patient information from a remote demographics supplier.

Turning on remote patient demographics supplier

The patient query interface functionality is available in the PACS appliance RIS interface. The Patient Demographics Supplier page only provides the configuration options for the remote patient demographics supplier.

After you turn on the remote patient demographics supplier, the Platform Service must be restarted for the changes to take effect.

To turn on a remote patient demographics supplier, perform the following steps.

1. Go to **Administration > Patient > Demographics Supplier**, and complete the following fields:
 - **Enable**: Turn on the query transaction to patient demographics supplier.
 - **Host Address**: Enter a valid IP address of the patient demographics supplier.
 - **Listening Port**: Enter a valid listening port of the patient demographics supplier.
 - **Sending Application**: Enter the sending application that is used for the HL7 query message by the client.
 - **Sending Facility**: Enter the sending facility that is used for the HL7 query message by the client.
 - **Receiving Application**: Enter the receiving application that is used for the HL7 query message by patient demographics supplier.
 - **Receiving Facility**: Enter the receiving facility that is used for the HL7 query message by patient demographics supplier.
2. Select **Save**. The Apply Changes and Restart Platform Service dialog displays.
3. Confirm the change, and then select **OK**. The changes are applied, and the Platform Service is restarted.

PIX Settings

From **Administration > Patient > PIX Settings**, turn on queries for patient identifier cross-referencing (PIX), and configure the PIX manager.

The PACS appliance supports patient identifier cross-referencing (PIX) as a PIX consumer actor. The system is able to query a PIX manager to get patient identifier information from other patient identification domains for an existing local patient.

Configuring PIX manager

To configure the PIX manager, perform the following steps.

1. Go to **Administration > Patient > PIX Settings > Manager** tab, and complete the following fields:
 - **IP Address:** Enter a valid IP address for the PIX manager actor.
 - **Listening Port:** Enter a valid listening port for the PIX manager actor.
 - **Sending Application:** Enter the sending application that is used for the HL7 query message by the PIX consumer.
 - **Sending Facility:** Enter the sending facility that is used for the HL7 query message by the PIX consumer.
 - **Receiving Application:** Enter the receiving application that is used by the HL7 query message by PIX manager.
 - **Receiving Facility:** Enter the receiving facility that is used by the HL7 query message by PIX manager.
2. Select **Save**. A message displays confirming the configuration is saved.

Turning on PIX queries

The PIX query utilizes standard HL7 communication. PIX queries can be performed manually from **Patients > Search** and adopted by the DICOM service for querying, retrieving, and storing DICOM objects.

To turn on PIX queries, perform the following steps.

1. Go to **Administration > Patient > PIX Settings > Settings** tab, and select any of the following options:
 - **Enable PIX for DICOM Query:** Turn on this option, and the DICOM FIND SCP will utilize PIX transactions to accomplish cross-domain queries. For example, when the FIND SCP receives a request with patient ID criteria from a remote AE in a different patient identification domain, it will first query the PIX manager to get the corresponding local patient ID, and then it will use this local ID to perform the internal search. If matching results are found, then the patient ID attributes in the responses will be replaced with the original ID from the query requester.
 - **Enable PIX for DICOM Retrieve:** Turn on this option, and the DICOM MOVE SCP will utilize PIX transactions to accomplish cross-domain retrieval. For example, when the MOVE SCP receives a patient-level retrieval request from a remote AE that belongs to a different patient identification domain, it will first query the PIX manager to get the corresponding local patient ID, and then it will use this local ID to locate the objects to be sent. If the request is not patient level, then MOVE SCP just uses the requested level and UID to locate the object. During C-STORE, if the destination AE is in a different patient identification domain than the local system, then the patient ID in each dataset will be replaced with the corresponding ID in the destination domain.
 - **Enable PIX for DICOM Storage:** Turn on this option, and the DICOM STORE SCP will utilize PIX transactions to accomplish cross-domain storage. For example, when the STORE SCP receives a study from a remote AE that belongs to a different patient identification domain, first it will query the PIX manager to get the corresponding local patient ID, and then it will apply this local ID to the dataset for registration and storage.
2. Select **Save**. A message displays confirming the configuration is saved.

ASTRA

From **Administration > ASTRA**, access the following modules:

- **ASTRA Service** - Configure the PACS appliance to access ASTRA™ Cloud.
- **ASTRA Peers** - Add and maintain ASTRA™ peers.

ASTRA Service

ASTRA™ Cloud by Candelis® is a cloud computing solution for medical imaging and reports. From **Administration > ASTRA > ASTRA Service**, configure the PACS appliance to use ASTRA Cloud and to share studies with other physicians and PACS appliance servers in a reliable and secure manner.

Configuring network settings to access ASTRA Cloud

To configure network settings to access ASTRA Cloud, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Service**. The **Server** tab displays current connection settings.
2. In the **Connection Settings** section, complete the following fields:
 - **Host Address**: Enter a valid host address for ASTRA Cloud.
 - **Port**: Enter the listening port of ASTRA Cloud.
3. Select **Save**. A message displays confirming the configuration changes are saved.

Turning on download redirection

It is recommended to turn on download redirection because objects that are stored in ASTRA Cloud are downloaded directly from their source.

Consider the following when working with download redirection:

- If this option is not turned on, downloading objects from ASTRA Cloud will continue to function; however, connection timeouts may occur if the data is too large.
- Disable download redirection if your firewall blocks S3.
- If you want to unblock ASTRA Cloud services, then contact technical support for guidance opening the proper domains.

To turn on download redirection, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Service > Server** tab, and select **Use Download Redirection**.
2. Select **Save**. A message displays confirming the configuration changes are saved.

Registering PACS appliance with ASTRA Service

From **Administration > ASTRA > ASTRA Service > Registration** tab, register the PACS appliance with ASTRA Cloud.

During the process of registering the PACS appliance with ASTRA Cloud, you will have the option to turn on various features that use ASTRA Cloud. Because these features require a license, you will only see the features for which your system has a license. Default configurations are used when you turn on a licensed feature.

To avoid network connection issues during PACS appliance registration, it is recommended to verify the following:

- DNS settings and network configuration. Go to **Administration > System > Network Settings**.
- Host address and port for the ASTRA service. Go to **Administration > ASTRA > ASTRA Service > Server** tab.

To register the PACS appliance with ASTRA Service, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Service > Registration** tab.
2. In the **Contact Information** section, complete the following required fields:
 - **Customer Name**
 - **Facility**
 - **Address**
 - **City**
 - **State/Province**
 - **Zip/Postal Code**
 - **Country**
 - **Contact Email**

- **Phone Number**
- 3. Select **Register**. The ASTRA Terms of Service Agreement displays.
- 4. Read, understand, and accept the terms by selecting **I accept the terms of the agreement**.
- 5. Select **Accept**.
 - The ASTRA Registration dialog displays if your system has licenses for features that use ASTRA Cloud.
 - A private key is generated.

Downloading private key for ASTRA Cloud

When you register a PACS appliance with ASTRA Cloud, the PACS appliance generates and stores a private key, which is used to encrypt and decrypt the data stored in ASTRA Cloud.

From **Administration > ASTRA > ASTRA Service > Private Key** tab, download the private key for safekeeping.

It is imperative that you store your private key in a safe, protected location. If your private key is lost, then you will not be able to access your data in ASTRA Cloud.

To download your private key for ASTRA Cloud, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Service > Private Key** tab.
2. Select **Download**.
3. Browse to the location where you want to save the file, and then select **Save**.

Restoring private key for ASTRA Cloud

To restore your private key, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Service > Private Key** tab.
2. Select **Choose File**, select the file, and then select **Open**.
3. Select **Restore**.

ASTRA Peers

Before a PACS appliance can share studies with other ASTRA Cloud peers, the peers must first be added to the PACS appliance.

Adding ASTRA Cloud peers

From **Administration > ASTRA > ASTRA Peers**, add ASTRA Cloud peers, which may be another PACS server or a user workstation.

To add an ASTRA Cloud peer, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Peers**.
2. Select **Add New**. The ASTRA Peer - ASTRA Account dialog displays.
3. Complete the following fields:
 - **Account**: Enter a valid ASTRA Cloud account username or email address.
 - **Description**: Enter a brief description or name for the ASTRA Cloud peer.
4. Select **Next**. The ASTRA Peer - Inbound Policy dialog displays. If you need to return to a previous page, select **Previous**.
5. Select **Accept Inbound Studies** to grant permission for the ASTRA peer to transfer studies to the PACS appliance, and then select **Next**. The ASTRA Peer - Outbound Policy dialog displays.
6. Select the default format of the study for outbound transfers to the ASTRA peer, and then select **Next**. The ASTRA Peer - Review dialog displays.
7. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
8. Review the configuration, and select **Finish**. A message displays confirming the ASTRA peer was added.

Editing information for ASTRA peers

From **Administration > ASTRA > ASTRA Peers**, edit information for ASTRA peers.

To edit information for an ASTRA peer, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Peers**.

2. In the row that includes the ASTRA peer that you want to edit, select **Edit**. The ASTRA Peer - ASTRA Account dialog displays.
3. Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. A message displays confirming the changes to the ASTRA peer information was saved.

Deleting ASTRA peers

From **Administration > ASTRA > ASTRA Peers**, delete ASTRA peers.

To delete an ASTRA peer, perform the following steps.

1. Go to **Administration > ASTRA > ASTRA Peers**.
2. In the row that includes the ASTRA peer that you want to delete, select **Delete**. The Delete ASTRA Peer dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the ASTRA peer was deleted.

Users

From **Administration > Users**, access the following modules:

- **User Management** - Define and maintain user accounts for the PACS web application.
- **Site Security Policy** - Configure security settings for all user accounts in the PACS web application.
- **Active Sessions** - View information related to users currently signed in to the PACS web application.

User Management

From **Administration > Users > User Management**, define and maintain user accounts for the PACS web application.

Changing administrator password

To change the administrator password, perform the following steps.

1. Go to **Administration > Users > User Management**.
2. In the row that includes the admin user account, select **Set Password**. The password dialog displays.
3. Complete the following fields:
 - **Current Password**: Enter the current administrator password. The initial password is **password** by default.
 - **New Password**: Enter the new administrator password.
 - **Re-enter Password**: Re-enter the new password.
4. Select **OK**.

Adding user accounts

From **Administration > Users > User Management**, add user accounts.

Filter the list of user accounts by entering a term in the **Filter** field.

To add a user account, perform the following steps.

1. Go to **Administration > Users > User Management**. The list of existing user accounts displays.
2. Select **Add New**. The Add User dialog displays.
3. Complete the following required fields:
 - **Username**: Enter the username for the account.
 - **Password**: Enter a valid password for the user account.
 - **Re-enter Password**: Re-enter the password.
 - **Full Name**: Enter the full name of the user.
 - **User role**: Select the role for the user account.
 - **Operator**: May be assigned access to all system modules, local AEs, and remote AEs.
 - **Physician**: May only be assigned access to local AEs.
4. From the **Select User Permissions** section, assign access to modules in the system by highlighting the item and selecting **Add** or **Remove** as appropriate.
5. From the **Select Permitted Local AEs** section, assign access to local AEs by highlighting the AE and selecting **Add** or **Remove** as appropriate.
6. From the **Select Permitted Remote AEs** section, assign access to remote AEs by highlighting the AE and selecting **Add** or **Remove** as appropriate.
7. Select **OK**. A message displays confirming the user account is saved.

Editing information for user accounts

From **Administration > Users > User Management**, edit information, including user role, for user accounts.

Filter the list of user accounts by entering a term in the **Filter** field.

To edit information for a user account, perform the following steps.

1. Go to **Administration > Users > User Management**. The list of existing user accounts displays.
2. In the row that includes the user account that you want to edit, select **Edit**. The Edit User dialog displays.
3. Change the password by selecting **Change Password**, and then in the **Password** field and **Re-enter Password** field, enter a valid password for the user account.
4. Change user account information in any of the fields, or change access permissions.
5. Select **OK**. A message displays confirming the user account is saved.

Unlocking user accounts

From **Administration > Users > User Management**, unlock user accounts for which sign-in attempts have exceeded the configured maximum number.

Filter the list of user accounts by entering a term in the **Filter** field.

To unlock a user account, perform the following steps.

1. Go to **Administration > Users > User Management**. The list of existing user accounts displays.
2. In the row that includes the user account that you want to unlock, select **Unlock**. The unlock user dialog displays.
3. Confirm the action, and then select **Yes**. The user account is unlocked.

Deleting user accounts

From **Administration > Users > User Management**, delete user accounts.

Filter the list of user accounts by entering a term in the **Filter** field.

To delete a user account, perform the following steps.

1. Go to **Administration > Users > User Management**. The list of existing user accounts displays.
2. In the row that includes the user account that you want to delete, select **Delete**. The Delete dialog displays.
3. Confirm the deletion, and then select **Yes**. The user account is deleted from the system.

Site Security Policy

From **Administration > Users > Site Security Policy**, configure security settings for all user accounts in the PACS web interface.

Configuring security settings for user accounts

To configure security settings for user accounts, perform the following steps.

1. Go to **Administration > Users > Site Security Policy**, and complete the following fields:
 - **Session Inactivity Timeout**: Enter the number in minutes that a user session will remain responsive after the last user interaction; the user session is automatically signed out when the inactivity exceeds the threshold that you set. Select **None** to turn off **Session Inactivity Timeout**.
 - **Password Expiration**: Enter the number in days when a user password will expire, and users will be required to change their password. Select **None** to turn off **Password Expiration**.
 - **Password Requirements**: Select the options to require when creating or updating a user account password.
 - **Minimum Password Length**: Enter the minimum number of characters required when creating or updating a user account password.
 - **Maximum Failed Sign-In Attempts**: Enter the maximum number of user sign-in attempts after which the user account is locked.
 - **Allow OEM Access**: Select to grant access for support personnel.
2. Select **Save**. A message displays confirming the configuration changes are saved.

Active Sessions

From **Administration > Users > Active Sessions**, view user session information, including the remote address from which users are connected and the last time any activity was detected.

Select **Refresh** to update the active sessions information.

Viewing active sessions

Go to **Administration > Users > Active Sessions**. All active sessions display.

Forcibly sign out a user by selecting **Terminate** next to the user session.

Data Management

From **Administration > Data Management**, access the following modules:

- **Local Storage** - View and manage storage devices (raw disks) and volumes, and configure settings for system storage.
- **ASTRA Storage** - View ASTRA™ Cloud storage details, and configure expiration settings for ASTRA™ Cloud storage.
- **Backup Service** - Define and maintain backup policies.
- **Data Retention** - Define and maintain data retention policies.
- **Auto Deletion** - Configure settings for auto deletion.
- **Storage Optimization** - Configure settings for storage optimization.
- **Live Migration** - Migrate data from a source PACS system to the PACS appliance with minimal downtime.

Local Storage

From **Administration > Data Management > Local Storage**, view and manage current storage devices (raw disks) and volumes, and configure settings for system storage.

When a new PACS system is shipped to a customer, it includes a permanent db volume that is automatically managed by the system and is always ready for use. Because the system automatically manages this volume, the **Manage** option does not display for the device, and you cannot edit, disable, eject, or remove the db volume.

Managing devices and volumes

From **Administration > Data Management > Local Storage > Devices and Volumes** tab, view and manage devices and volumes.

When you install the PACS software on a virtual machine (VM), you provide a virtual disk (device) that is connected to the VM. This device (raw disk) displays in the **Devices** section, and the **Manage** option is available to create volumes on the disk. The system automatically creates the device name, such as sda, sdb, sdc. Volumes have a maximum of 16 TB. If the disk is greater than 16 TB, then the system creates more than one volume; if the disk is less than 16 TB, then the system only creates one volume. Each volume that is created by the system displays in the **Volumes** section with a name, such as v1, v2, v3, that is automatically created by the system.

To manage a device and its volume(s), perform the following steps.

1. Go to **Administration > Data Management > Local Storage > Devices and Volumes** tab.
2. Provide a virtual disk, and then select **Manage**. The system creates one or more volumes, depending on the size of the disk, and the volume displays in the **Volumes** section. The **Manage** option is no longer available for that device.
3. In the **Volumes** section, format the volume by selecting the volume row and then selecting **Format**. The volume is automatically formatted, mounted, and ready for use. The status displays **Enabled**, **Mounted**, **Ready**, and the **Format** option is no longer available for that volume.
4. Perform additional actions for a highlighted volume by selecting any of the following options:
 - **Disable**: Take down a volume. This may be useful if you need to perform maintenance on the volume or to troubleshoot an issue with the volume.
 - **Eject Media**: Eject a removable media, such as a USB drive that you are using for external storage.
 - **Remove**: Remove a volume from use.

Specifying storage types for volumes

When you add a new volume to the system, specify the type of storage, including DICOM studies, RIS attachments, and rendering, for which the volume will be used. If a volume is greater than a specific size, then all the storage types are automatically selected when the volume is created by the system. If the volume is less than a specific size, then you must specify the storage type.

Note that the db volume is typically small, such as 65 GB, so storage types are not automatically assigned to this permanent volume.

To specify storage types for a volume, perform the following steps.

1. Go to **Administration > Data Management > Local Storage > Devices and Volumes** tab.
2. In the **Volumes** section, select the volume for which you want to specify a storage type, and then select **Edit**. The Choose Storage Type dialog displays.
3. Select one or more storage type, depending on the size of the volume, and then select **Save**. A message displays confirming the configuration changes are saved.

Configuring storage settings

From **Administration > Data Management > Local Storage > Storage Settings** tab, configure settings, such as storage reserves, storage thresholds, and storage reclamation, for all storage devices on the system to ensure a minimum amount of free space is maintained and always made available for normal system operations.

View real-time system usage from the default **Dashboard** and the **Performance Dashboard**.

To configure settings for system storage, perform the following steps.

1. Go to **Administration > Data Management > Local Storage > Storage Settings** tab.
2. In **Reserved Storage Settings**, complete any of the following fields:
 - **System Reserved Space**: Enter the amount of space in GB that is reserved on each volume for normal system operations.
 - **Database Reserved Space**: Enter the amount of space in GB that is reserved on the head unit for database storage.
3. In **Storage Threshold Settings**, complete any of the following fields:
 - **Free Space Threshold**: Enter the amount of free disk space in GB that the system will try to maintain under normal operating conditions. Data purging must be turned on in the **Storage Reclamation Settings** section for the threshold to be triggered.
 - **Critical Space Threshold**: Enter the critical disk space threshold in GB in which the system will begin to take emergency actions. Data purging must be turned on in the **Storage Reclamation Settings** section for the threshold to be triggered.
4. In **Storage Reclamation Settings**, select **Enable Data Purging** to turn on data purging.
5. Select **Save**. A message displays confirming the configuration is saved.

ASTRA Storage

From **Administration > Data Management > ASTRA Storage**, view ASTRA™ Cloud storage details, and configure expiration settings for ASTRA™ Cloud storage.

You must have a license to use the ASTRA™ Service. Contact your sales representative if you want to purchase an ASTRA™ Service license for your PACS system.

Configuring expiration settings for ASTRA Cloud storage

Changes made to expiration settings will not apply to data that are already stored in ASTRA™ Cloud.

View ASTRA™ Cloud storage usage and shared objects from **Administration > Data Management > ASTRA Storage > Storage Usage** tab.

To configure expiration settings for ASTRA™ Cloud storage, perform the following steps.

1. Go to **Administration > Data Management > ASTRA Storage > Storage Detail** tab.
2. In **Expiration Settings** complete any of the following fields:
 - **Backup Expiration**: Enter the number in years that backup objects should remain in ASTRA™ Cloud storage.
 - **Share Expiration**: Enter the number in days that shared objects should remain in ASTRA™ Cloud storage.
3. Select **Save**. A message displays confirming the configuration is saved.

Backup Service

From **Administration > Data Management > Backup Service**, define and maintain backup policies.

You must have a backup destination license to use the Backup Service. Contact your sales representative if you want to purchase a backup destination license for your PACS system.

Turning on backup services

The Backup Service creates duplicate copies of various data objects to the secondary storage. When the Backup Service is turned on, the PACS appliance backs up to secondary storage all DICOM studies, attachments, configuration files, and its internal database.

To turn on backup services, perform the following steps.

1. Go to **Administration > Data Management > Backup Service**. The **Settings** tab displays.

2. Complete the following fields:
 - **Enable:** Select to turn on backup services. If you do not have a license for Backup Service, this service will not function when you turn it on.
 - **Restrict:** Select to restrict backup during business hours. Business hours are configured in **Administration > System > General Settings**.
 - **Delay:** Enter the time in seconds that the backup occurs after a study arrives.
3. Select **Save**. A message displays confirming the configuration is saved.

Adding backup policies

From **Administration > Data Management > Backup Service > Policies** tab, add backup policies.

Only licensed backup destinations will be available for selection when adding a backup policy.

To add a backup policy, perform the following steps.

1. Go to **Administration > Data Management > Backup Service > Policies** tab.
2. Select **Add New**. The Add Backup Policy - Source AEs dialog displays.
3. Select the source AEs that contain the studies to be backed up, and then select **Add**. Select **Do not backup studies** if the backup policy is intended only to back up system files.
4. Select **Next**. The Add Backup Policy - Study Criteria dialog displays.
5. Select the study criteria that determines which studies will be backed up, and then select **Next**. The Add Backup Policy - System Files dialog displays.
6. Select the type of system files to back up, and then select **Next**. The Add Backup Policy - Backup Destination dialog displays.
7. Select the backup destination, and then select **Next**. The Add Backup Policy - Description dialog displays.
8. In the **Description** field, enter a description for the backup policy, and then select **Next**. The Add Backup Policy - Review dialog displays.
9. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
10. Review the configuration, and select **Finish**. A message displays confirming the policy is saved, the backup policy is added, and the **Status** column displays **Disabled**.
11. Select **Enabled**, and the policy status changes to **Enabled**.

Turning off backup policies

To turn off a backup policy, perform the following steps.

1. Go to **Administration > Data Management > Backup Service > Policies** tab.
2. In the row that includes the backup policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Editing information for backup policies

To edit backup policy information, perform the following steps.

1. Go to **Administration > Data Management > Backup Service > Policies** tab.
2. In the row that includes the backup policy that you want to edit, select **Edit**. The Edit Backup Policy - Source AEs dialog displays.
3. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. A message displays confirming the policy is saved.

Deleting backup policies

To delete a backup policy, perform the following steps.

1. Go to **Administration > Data Management > Backup Service > Policies** tab.
2. In the row that includes the backup policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion, and then select **Yes**. The backup policy is removed.

Data Retention

From **Administration > Data Management > Data Retention**, define and maintain policies for retaining data.

Based on HIPAA and other regulations, studies may not be required to be kept permanently. Data retention policies allow you to specify for how long different data should be stored on the PACS appliance before they can be permanently deleted. This feature is available only if the PACS appliance is not configured as a cache router.

Adding data retention policies

From **Administration > Data Management > Data Retention**, add policies for retaining data.

One or more data retention policies can be added to apply different retention criteria for different studies; however, it is not recommended to define multiple policies that have overlap on the same group of studies. If such policies are defined, as long as a study qualifies for the deletion criteria from any policy, the study will be permanently deleted.

To add a data retention policy, perform the following steps.

1. Go to **Administration > Data Management > Data Retention**.
2. Select **Add New**. The Add Data Retention Policy - Source AEs dialog displays.
3. Select specific source AEs or all AEs that include the studies to be deleted, and then select **Next**. The Add Data Retention Policy - Date Criteria dialog displays. If you need to return to a previous page, select **Previous**.
4. Select the time constraints for study date, study arrival date, and last accessed date to determine whether a study is qualified for deletion, and then select **Next**. The Add Data Retention Policy - Study Criteria dialog displays.
5. Configure study criteria for deletion, and then select **Next**. The Add Data Retention Policy - Description dialog displays.
6. In the **Description** field, enter a brief description or name for the policy, and then select **Next**. The Add Data Retention Policy - Review dialog displays.
7. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
8. Review the configuration, and select **Finish**. A message displays confirming the policy is saved, and the **Status** column displays **Enabled**.

Turning off policies for data retention

To turn off a data retention policy, perform the following steps.

1. Go to **Administration > Data Management > Data Retention**.
2. In the row that includes the data retention policy that you want to turn off, select **Disable**. The **Status** column displays **Disabled**.
3. To turn on a disabled policy, select **Enable**. The **Status** column displays **Enabled**.

Editing information for data retention policies

To edit data retention policy information, perform the following steps.

1. Go to **Administration > Data Management > Data Retention**.
2. In the row that includes the data retention policy that you want to edit, select **Edit**. The Edit Data Retention Policy - Source AEs dialog displays.
3. (Optional) Change information you entered on a page by selecting the name of the page in the left pane, modifying the information, and then selecting **Review** in the left pane. The Review page displays.
4. Review the configuration, and select **Finish**. A message displays confirming the policy is saved.

Deleting backup policies

To delete a data retention policy, perform the following steps.

1. Go to **Administration > Data Management > Data Retention**.
2. In the row that includes the data retention policy that you want to delete, select **Delete**. The Delete Policy dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the data retention policy is deleted.

Auto Deletion

From **Administration > Data Management > Auto Deletion**, delete the oldest studies when eligible online storage falls below the configured watermark. This feature is available only if the PACS appliance is configured as a cache router.

Configuring settings for auto deletion

To configure the settings for auto deletion, perform the following steps.

1. Go to **Administration > Data Management > Auto Deletion > Configuration** tab.
2. Complete the following fields:
 - **Auto Delete By:** Specify the criteria that will be used to determine the oldest studies. Select either **Last Access Date** or **Study Date**.
 - **Minimal Eligible Space:** Specify the minimum amount of eligible free space that will be maintained under heavy usage conditions. During heavy usage, the amount of eligible disk space may fall below the nominal eligible space threshold, but this minimum eligible space will be maintained until operating conditions return to normal.
 - **Nominal Eligible Space:** Specify the amount of eligible free disk space that will be maintained under normal operating conditions at the scheduled time. It must be configured larger than **Minimal Eligible Space**.
3. Select **Save**.

Storage Optimization

From **Administration > Data Management > Storage Optimization**, compress online studies stored on the PACS appliance to reclaim storage space. The compression ratio varies, depending on the type of imaging data and the algorithm used.

Configuring settings for storage optimization

From **Administration > Data Management > Storage Optimization > Configuration** tab, configure storage optimization by selecting a compression algorithm.

The compression algorithms may include, but not be limited to, the following options:

- **JPEG-2000 Lossless**
- **JPEG-LS Lossless**
- **JPEG Lossless**
- **RLE Lossless**
- **Deflated Explicit Little Endian**
- **JPEG-2000 Lossy**
- **JPEG-LS Lossy**

Consider the following when configuring storage optimization:

- Be extremely cautious about using lossy compression algorithms. The image quality will degrade, and it is not recoverable.
- Only imaging data will be compressed. If the image is already in a compressed format, no further compression or conversion will be performed.

To configure the settings for storage optimization, perform the following steps.

1. Go to **Administration > Data Management > Storage Optimization > Configuration** tab.
2. Select **Enable** to turn on compression.
3. From the **Compression Algorithm** dropdown list, select the algorithm.
4. Select **Save**.

Scheduling storage optimization services

First enable the storage optimization service from **Administration > Data Management > Storage Optimization > Configuration** tab, and then configure the scheduled run time to start the service.

To schedule the storage optimization service, perform the following steps.

1. Go to **Administration > Data Management > Storage Optimization > Schedule** tab.
2. Complete the following fields:
 - **Scheduled Time:** Select the hour and minute when the compression will start.
 - **Scheduled Days:** Select the day or days of the week when compression will occur.
3. Select **Save**.

Live Migration

From **Administration > Data Management > Live Migration**, initiate live migration to move data from an existing source Candelis PACS system to another Candelis PACS appliance. Unlike the standard method of migrating data, live migration allows users to query and retrieve any existing studies through the DICOM interface, even while the studies are actively being migrated from one system to the other.

Full migration requires an activation license and only works with Candelis PACS appliance servers. Contact technical support if you need to activate a migration license.

Understanding live migration

The live migration process can be separated into three related, but independent, stages:

- **Verification:** During this phase, the PACS appliance verifies the settings to ensure the PACS appliance and the source PACS system are configured correctly. If an error is detected, the entire migration process is stopped. This stage can be skipped when **Enable Verification** is not turned on from **Administration > Data Management > Live Migration > Configuration** tab.
- **Indexing:** PACS appliance queries the source PACS system to initialize the database records required for live migration. The PACS appliance will be inactive for the duration of the indexing phase.
- **Data migration:** Data is actively migrated from the source PACS system to the PACS appliance. During this phase, users may query and retrieve studies on the source PACS system via the DICOM interface of the PACS appliance.

Configuring settings for live migration

From **Administration > Data Management > Live Migration > Configuration** tab, configure general settings and configure settings for indexing and migration.

Full migration requires an activation license and only works with PACS appliance servers. Contact technical support if you need to activate a migration license.

To configure settings for live migration, perform the following steps.

1. Go to **Administration > Data Management > Live Migration > Configuration** tab.
2. Select a migration method.
3. In **General Settings**, complete the following fields:
 - **Source Host Address:** Enter a valid host address for the source system.
 - **Dedicated AE Title:** Enter the remote AE title added to the source system.
 - **Enable Verification:** Select to turn on basic verification before performing database indexing and data migration.
4. In **Indexing Settings**, complete the following fields:
 - **Maximum Queries per Association:** Enter the maximum number of C-FINDs made per association.
 - **Pause Before Committing:** Select for the system to wait for user action before committing database indexing and starting data migration.
 - **Indexing Level:** From the dropdown list, select the type of database records to be built during the indexing stage. Selecting study-level indexing will speed up the entire indexing process; however, selecting instance-level indexing will provide more details in the migration report.
5. In **Migration Settings**, complete the following fields:
 - **Local Port:** Enter the DICOM port used exclusively for migrating data. This entry must be different than the normal DICOM port used by PACS appliance.
 - **Maximum Concurrent Retrieve Requests:** Enter the maximum number of concurrent retrieve requests made.
 - **Reserved for Transparent Retrieve:** Enter the number of transparent retrieve requests to be reserved.
6. Select **Save**.

Initiating live migration

From **Administration > Data Management > Live Migration > Migration** tab, add all the application entities from the existing PACS system that will be migrated, and then initiate live migration.

To initiate the live migration process, perform the following steps.

1. Disconnect the Ethernet cable from the network interface of the existing PACS system, such as the source system from where data is to be migrated.
2. Connect the Ethernet cable to the first network interface of the PACS appliance.
3. Use a separate Ethernet cable to connect the source PACS system to the second network interface of the PACS appliance.
4. Register the following application entity in the source PACS system by entering the following values:
 - **Dedicated AE Title:** IGMigrate
 - **Source Host Address:** 192.168.0.1
 - **Source Port:** 4001
5. Change the static IPv4 address of the source PACS system to 192.168.0.2.
6. Go to **Administration > Data Management > Live Migration > Migration** tab.
7. Select **Add New**. The Add Source AE dialog displays.
8. In the **Source AE** field, enter the name of the source AE, and then select **OK**.

9. Add all the AEs needed for migration.
10. Start live migration by selecting **Start Migration**.
11. During live migration, select any of the following actions as needed:
 - **Abort**: Abort the indexing.
 - **Resume**: Resume the verification or indexing upon failure.
 - **Skip**: Skip part of indexing when applicable.
 - **Commit**: Commit indexing at the end if the **Pause Before Committing** is turned on in from **Administration > Data Management > Live Migration > Configuration** tab > **Indexing Settings**.
 - **Retry**: If any studies fail to migrate, then the **Retry** option will be available. Select to retry migrating the failed studies.
12. Track the progress of live migration, including viewing the migration status for each application entity of the existing PACS system.
13. Select **Complete Migration** when data migration is complete, regardless of whether all studies were successfully migrated. A live migration report is generated for each migrated application entity.
14. Download a report for each migrated AE by selecting the **Report** icon in the row of the migrated AE.

Tracking progress of live migration

From **Administration > Data Management > Live Migration > Migration** tab, monitor and view the migration status for each application entity of the existing PACS system. This migration status will be automatically refreshed during live migration.

Live migration progresses through the following statuses:

- **Error**: An error occurred.
- **Pending**: Pending for verification.
- **Verifying**: Verifying the settings.
- **Verified**: The settings have been verified.
- **Indexing**: Indexing the database records.
- **Indexed**: The database records are indexed.
- **Migrating**: Migrating the studies.
- **Migrated**: All studies discovered are migrated or unable to be migrated.
- **Reporting**: Creating the migration report.
- **Completed**: Migration is complete.

Select **Refresh Log** to view the current migration log for the overall migration process or to view any error log messages.

Deleting AEs from live migration

To delete an AE from live migration, perform the following steps.

1. Go to **Administration > Data Management > Live Migration > Migration** tab.
2. In the row that includes the AE that you want to delete, select **Delete**. The Delete Local AE dialog displays.
3. Confirm the deletion, and then select **Yes**. The AE is deleted.

XDS

From **Administration > XDS**, access the following modules:

- **XDS Service** - Configure settings for XDS service.
- **XDS Registry** - Configure settings for XDS registry.
- **XDS Repository** - Configure settings for XDS repository.

XDS Service

From **Administration > XDS > XDS Service**, configure settings for XDS service.

Configuring settings for XDS service

From **Administration > XDS > XDS Service**, configure the listening port at which to accept incoming XDS transactions. By default, the system will listen on port 9191 for connections.

To configure settings for XDS service, perform the following steps.

1. Go to **Administration > XDS > XDS Service**.
2. Complete the following fields:
 - **Listening Port**: Enter the listening port for incoming XDS transactions.
 - **Secure Listening Port**: Enter the secure listening port.
 - **Secure Transfer Certificate**: Select the secure transfer certificate from **Administration > System > Certificates > Peer Certificates** tab.
3. Select **Save**.

XDS Registry

From **Administration > XDS > XDS Registry**, configure the settings for the XDS registry.

Configuring settings for XDS registry

From **Administration > XDS > XDS Registry**, configure the settings for the XDS registry.

The **Non-Secure Endpoint Address** and **Secure Endpoint Address** URLs that display on this page are the URLs that other XDS actors will need to use when sending transactions to your XDS registry.

To configure settings for XDS registry, perform the following steps.

1. Go to **Administration > XDS > XDS Registry**.
2. Select **Enabled** to turn on the XDS registry. If clear, the system will reject all XDS transactions intended for a registry actor.
3. From the **Patient Identification Domain** dropdown list, select a domain.
4. Select **Save**.

XDS Repository

From **Administration > XDS > XDS Repository**, configure the settings for the XDS repository.

Configuring settings for XDS repository

From **Administration > XDS > XDS Repository**, configure the settings for the XDS repository.

The XDS repository must register all documents it receives with an XDS registry.

- If the same PACS appliance is acting both as the repository and as the registry, get the endpoint address URL from **Administration > XDS > XDS Registry** page.
- If another appliance is acting as the registry, then contact the registry vendor to get the endpoint address URL, or consult vendor documentation as needed.

The **Non-Secure Endpoint Address** and **Secure Endpoint Address** URLs that display on this page are the URLs that other XDS actors will need to use when sending transactions to your XDS registry.

To configure settings for XDS repository, perform the following steps.

1. Go to **Administration > XDS > XDS Repository**.
2. Select **Enabled** to turn on the XDS repository. If clear, the system will reject all XDS transactions intended for a repository actor.
3. In the **Unique ID** field, enter the unique identifier for the XDS repository. All actors in an XDS workflow should be assigned a unique identifier; this is typically determined by the site.
4. In the **Endpoint Address of Registry** field, enter the URL for the XDS registry.
5. Select **Save**.

Patients

From **Patients**, access the following modules:

- **Search:** Search for existing patient records, and access functionality for viewing and working with patient records.
- **Conflicts:** Search for existing patient records that have the same patient ID, and access functionality for viewing and working with these patient records.
- **Create Patient:** Create a patient record.
- **CD/DVD:** Export and import patient record data via CD/DVD media.
- **Bulk Import:** Import a bulk set of patient records into the system.

When **Veterinary Mode** is turned on in **Administration > System > Applications Settings > Web Administration Options** tab, then veterinary-specific fields are available for creating veterinary patient records in **Patients > Create Patient**. When veterinary records exist in the system, you are able to search for them from **Patients > Search** and **Patients > Conflicts**.

Working with veterinary patient records and study records is the same as working with human patient and study records.

Search

From **Patients > Search**, search for existing patient records, and for the patient records that display, perform any of the following tasks:

- Open patient records to [view information related to the patient](#), including studies performed, and [edit patient demographics information](#).
- [Export patient studies](#), and remove current studies from the worklist.
- [Delete patient records](#).
- [Merge two patient records](#) that have the same patient demographics information into a single patient record.
- [Link two patient records](#).
- [Query the PIX manager](#).

Searching for existing patient records

Before you are able to work with a patient record, first search for the record from **Patients > Search**.

To search for a patient record, perform the following steps.

1. Go to **Patients > Search**, and complete any of the following fields:
 - **Patient ID:** Enter the primary identification number for the patient.
 - **Patient's Name:** Enter the name of a specific patient.
 - **Sex:** Select the sex of the patient.
 - **Date of Birth:** Select a date from the calendar date picker.
2. Select **Search**. The patient records that match the criteria display, and a message confirms the number of records that match the criteria. Any patient records that are not designated as the main patient record appear dim in the search results.
3. Navigate page results of patient records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Searching for existing veterinary patient records

When **Veterinary Mode** is turned on in **Administration > System > Applications Settings > Web Administration Options** tab, then you are able to search for veterinary patient records from **Patients > Search**.

To search for a veterinary patient record, perform the following steps.

1. Go to **Patients > Search**, and complete any of the following fields:
 - **Patient ID:** Enter the primary identification number of a specific veterinary patient.
 - **Patient's Name:** Enter the name of a specific veterinary patient.
 - **Sex:** Select the sex of the veterinary patient.
 - **Species:** Enter the species of the veterinary patient.
 - **Breed:** Enter the breed of the veterinary patient.
 - **Responsible Person:** Enter the name of the person with medical decision-making authority for the veterinary patient.
2. Select **Search**. The veterinary patient records that match the criteria display, and a message displays the number of records that match the criteria.

3. Navigate page results of veterinary patient records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Viewing details of patient records

From **Patients > Search**, search for a patient record, and then open the record to view its details, including patient demographics, associated studies, any conflicting patient records, and linked patient records.

To view details of a patient record, perform the following steps.

1. Go to **Patients > Search**, and search for a patient record. The patient records that match the criteria display.
2. In the row that includes the record of which you want to view details, select the **Open** folder icon. The Patient Details page displays the following sections:
 - **Patient Demographics.** Includes patient details, such as patient names and telephone number.
 - **Studies.** Includes studies belonging to this specific patient.
 - **Patient Conflicts.** Lists all patient records that share the same patient ID, but have a different first name or last name, or date of birth, or sex.
 - **Linked Patients.** Lists patient records that are linked to the current patient record.
3. Select **Back to Search** to close the Patient Details page and redisplay the Search page results.

Conflicts

From **Patients > Conflicts**, search for conflicting patient records, which include patient records that share the same patient ID, but have a different first name or last name, or date of birth, or sex. For the patient records that display, perform any of the following tasks:

- Open patient records to [view information related to the patient](#), including studies performed, and [edit patient demographics information](#).
- [Export patient studies](#), and remove current studies from the worklist.
- [Delete patient records](#).
- [Merge two patient records](#) that have the same patient demographics information into a single patient record.
- [Link two patient records](#).
- [Query the PIX manager](#).

The parameters for evaluating conflicts in patient data are configured from **Administration > Patient > Quality Control > Conflict Control** tab.

Searching for patient records with conflicting data

To search for patient records with conflicting data, perform the following steps.

1. Go to **Patients > Conflicts**, and complete any of the following fields:
 - **Patient ID:** Enter the primary identification number for the patient.
 - **Patient's Name:** Enter the name of a specific patient.
 - **Sex:** Select the sex of the patient.
 - **Date of Birth:** Select a date from the calendar date picker.
2. Select **Search**. The patient records that match the criteria display, and a message displays the number of records that match the criteria.
3. Navigate page results of patient records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Searching for veterinary patient records with conflicting data

When **Veterinary Mode** is turned on in **Administration > System > Applications Settings > Web Administration Options** tab, then you are able to search for veterinary patient records that have conflicting data.

To search for veterinary patient records with conflicting data, perform the following steps.

1. Go to **Patients > Conflicts**, and complete any of the following fields:
 - **Patient ID:** Enter the primary identification number of a specific veterinary patient.
 - **Patient's Name:** Enter the name of a specific veterinary patient.
 - **Sex:** Select the sex of the veterinary patient.
 - **Species:** Enter the species of the veterinary patient.
 - **Breed:** Enter the breed of the veterinary patient.

- **Responsible Person:** Enter the name of the person with medical decision-making authority for the veterinary patient.
- 2. Select **Search**. The veterinary patient records that match the criteria display, and a message displays the number of records that match the criteria.
- 3. Navigate page results of veterinary patient records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Resolving conflicts in patient data

From **Patients > Conflicts**, resolve conflicts in patient records that have the same patient ID. The process for resolving conflicting patient records is similar to the process for merging patient records. When you resolve the conflict, the two patient records that have the same patient ID are merged into a single patient record, and the patient record that you first selected is deleted from the system.

Access the resolving conflicts functionality directly from the **Patients > Conflicts** search results page, from the **Patients > Search** results page, or from the **Patient Details** page.

To resolve conflicts in patient data, perform the following steps.

1. Go to **Patients > Conflicts**, and view details of the patient record for which you want to resolve conflicting data.
2. In the **Patient Conflicts** section, select **Resolve**. The Resolve Patient Conflicts dialog displays the record that you selected and any additional records that include the same patient ID.
3. Select the patient record to which you want to merge the current patient record, and then select **Next**. The Resolve Patient Conflicts dialog displays the original patient demographics information and the proposed patient demographics.
4. Confirm you want to resolve the conflict, and then select **Finish**. The patient data is merged into the record, and the original patient record is deleted.
5. Select **Back to Search** to close the Patient Details page and redisplay the Conflicts search results page.

Create Patient

From **Patients > Create Patient**, create patient records.

Creating patient records

When **Veterinary Mode** is turned on in **Administration > System > Applications Settings > Web Administration Options** tab, then fields for **Patient Species Description**, **Patient Breed Description**, and **Responsible Person** also display.

Name fields have the following parameters:

- Maximum 64 characters
- Backslash ('\') is not allowed
- Either a first name or a last name is required to complete to save a patient record.

To create a patient record, perform the following steps.

1. Go to **Patients > Create Patient**.
2. Complete the following **Patient Identification** fields:
 - **Patient ID:** (Required) Enter the primary identification number for the patient.
 - **Prefix:** Enter a prefix for the patient name.
 - **First Name:** (Required) Enter a first name for the patient.
 - **Middle Name:** Enter a middle name for the patient.
 - **Last Name:** (Required) Enter a last name for the patient if you did not enter a first name for the patient.
 - **Suffix:** Enter a suffix for the patient name.
 - **Patient's Sex:** (Required) Select the sex of the named patient.
 - **Patient's Birth Date:** (Required) Select a date of birth from the calendar date picker for the named patient.
 - **Patient's Birth Time:** Select a time of birth from the calendar date picker for the named patient.
3. Complete any of the following optional **Other Information** fields:
 - **Patient ID Issuer:** Enter the identifier of the Assigning Authority that issued the patient ID.
 - **Other Patient IDs:** Enter other identification numbers or codes that may be used to identify the patient.
 - **Other Patient Names:** Enter other names that may be used to identify the patient.
 - **Ethnic Group:** Enter an ethnic group or race of patient.
 - **Medical Alerts:** Enter medical conditions to which medical staff should be alerted.
 - **Allergies:** Enter a description of prior reaction to contrast agents or other patient allergies or adverse reactions.
 - **Patient's Telephone Number:** Enter a telephone number where the patient can be reached.
4. Select **Save**. A message displays confirming the new patient record is saved.

- If a patient record already exists with the same patient ID, then the Confirm Patient Edit dialog displays. Select **No**, and the duplicate patient record is not saved.
- If a patient record already exists with the same patient ID, then the Confirm Patient Edit dialog displays. Select **Yes** if you want to save the patient record with the duplicate patient IDs. A message confirms the record is saved.

Editing information in patient records

From **Patients > Search**, edit information in a patient record.

When editing patient records, both the patient information and the studies for this patient in the system will be modified with the new patient information.

To edit information in a patient record, perform the following steps:

1. Go to **Patients > Search**, and view details of the patient record. The Patient Details page displays.
2. In the **Patient Demographics** section, select **Edit Patient**. The Edit Patient Details dialog displays.
3. Edit information in any of the fields, and then select **OK**. The Confirm Patient Edit dialog displays.
4. Perform any of the following actions, depending on the change made.
 - If one or more patients with the same patient ID exists, confirm you want to make the change, and then select **Yes**. The Confirm Patient Edit dialog displays.
 - If the changes to the patient demographics information match an existing patient record, then the Merge Patient dialog displays. If you want to merge the patient records, then select **Yes**. If you do not want to merge patient records, then select **No**. Modify patient information, and select **OK**.
5. Confirm you want to save changes made to all studies for the patient, and then select **Yes**. A message displays confirming the changes are saved.
6. Select **Back to Search** to close the Patient Details page and redisplay the Search page results.

Merging patient records

From **Patients > Search**, merge two patient records that have the same patient demographics information, such as patient ID, last name, first name, sex, and birth date, into a single patient record. The patient record that you first select will be deleted.

Access the merge functionality directly from the Search results page or from the Patient Details page.

To merge a patient record, perform the following steps.

1. Go to **Patients > Search**, and search for a patient record. The patient records that match the criteria display.
2. Select the record that you want to merge into another record, and then select **Merge**. The Merge Patient dialog displays any records that have the same patient ID.
3. (Optional) Enter patient demographics information into the fields, and then select **Search**. The record that matches the patient information displays.
4. In the list of records, select the record to which you want to merge the current patient record, and then select **Next**. The Merge Patient dialog displays the original patient demographics and the proposed patient demographics.
5. Review the data, and then select **Finish**. A message displays that the patient records were merged into a single record, and the original patient record is deleted.

Exporting patient studies to CD/DVD export worklist

From **Patients > Search**, export all the studies of a single patient to the CD/DVD export worklist. From the CD/DVD export worklist, you are able to copy (burn) the studies to a CD or DVD.

Access the export studies functionality directly from the Search results page or from the Patient Details page.

To export patient studies to the CD/DVD export worklist, perform the following steps.

1. Go to **Patients > Search**, and search for a patient record. The patient records that match the criteria display.
2. In the row that includes the study that you want to export, select the **Burn Media** icon. The Export Patient Studies dialog displays.
3. Confirm you want to remove the studies from the current worklist and export the studies to the CD/DVD export worklist, and then select **Yes**. The studies are added to the CD/DVD export worklist, and the **Patients > CD/DVD** page opens and displays the studies that you exported.

For information how to export studies, go to [Exporting patient studies to CD/DVD](#).

Linking patient records

From **Patients > Search**, link two or more patient records together. When you link multiple patient records, you must do the following:

- Designate one record as the main patient record.
- Rearrange three or more records, as needed, to designate one record as a main record.

When records are linked, any patient records that are not marked as a main record will be will appear dim in the patient Search results.

To link two or more patient records together, perform the following steps.

1. Go to **Patients > Search**, and search for a patient record. The patient records that match the criteria display.
2. Select the patient record that you want to link to another record, and then select **Link**. The Link Patient dialog displays all the patient records in the system.
3. (Optional) Enter patient demographics information into the fields, and then select **Search**. The records that match the patient information display.
4. In the list of records, select the patient record to which you want to link, and then select **Next**. The Link Patient dialog displays the group of linked patient records.
5. If the records are already part of a group of linked records, then rearrange the records into groups, if needed, and then select **Next**.
6. Select the patient record that is the main patient record of a group.
7. Select **Finish**. The patient records are linked, and any non-main patient record field labels appear dim.

Unlinking patient records

From **Patients > Search**, unlink patient records.

1. Go to **Patients > Search**, and view details of the patient record that you want to unlink. The Patient Details page displays.
2. In the **Linked Patients** section, select **Unlink**. The Unlink Patient dialog displays all the linked patient records in the group.
3. Select one or more patient records to unlink, and then select **Finish**. A message displays confirming the records are unlinked.
4. Select **Back to Search** to close the Patient Details page and redisplay the Search page results.

Querying PIX manager

From **Patients > Search**, retrieve patient identifiers from other patient identification domains using the PIX manager.

To query the PIX manager, perform the following steps.

1. Go to **Patients > Search**, and search for a patient record. The patient records that match the criteria display.
2. Select the patient record for which you want to query the PIX manager, and then select **Query PIX**.
3. From the **Query Pix** dropdown list, select one or more PIX domains on which to search, and then select **Query**. If you do not select a domain, then all the domains will be queried. The Query Pix Manager dialog displays the query results.
4. Select **Close**.

Deleting patient records

If the system is licensed with ImageGrid[®] Platform and the patient record includes ImageGrid Platform data that are related to this patient, then the patient record cannot be deleted from this PACS appliance.

To delete a patient record, perform the following tasks.

1. Go to **Patients > Search**, and search for existing patient records.
2. Select one or more patient records that you want to delete. The **Delete** option becomes available to select.
3. Select **Delete**. The Delete Patient Data Permanently dialog displays the following message: **Warning: Deleting patient will delete all the studies across all AE titles. The data will not be recoverable.**
4. Confirm that you want to delete the patient record and the data across all AEs, and then select **Yes**. A message displays that the record was successfully deleted.

CD/DVD

From **Patients > CD/DVD**, import and export patient studies via CD/DVD media.

Studies that have been exported from **Patients > Search** or **Patients > Conflicts** are automatically moved to the CD/DVD worklist.

Exporting study data to a CD/DVD is not intended for use as a backup mechanism; use the Backup Service configured from **Administration > Data Management > Backup Service**.

Exporting patient studies to CD/DVD

From **Patients > CD/DVD > Export** tab, export selected studies for a single patient to a DICOMDIR CD/DVD.

To export studies to a DICOMDIR CD/DVD, perform the following steps.

This procedure assumes that you have already exported the patient studies from a Search results page to the CD/DVD worklist.

1. Insert a recordable CD or DVD media into the optical drive of the PACS appliance.
2. Go to **Patients > CD/DVD > Export** tab.
 - Studies that have been exported to the CD/DVD worklist display. If the study that you want to export does not display, select **Select New Patient**, and perform a search for the patient record.
 - The **Status** field displays **Available** if the disk is compatible and recordable.
3. Select the studies to burn to the CD. The size of the exported studies will be updated as studies are selected. If the total size exceeds the capacity of the disk, burning the studies will not be allowed.
4. Select **Burn Media**. The recording process starts. When the burning process is complete, the CD/DVD will be ejected automatically.
5. Select **Clear Study List** to remove the current studies from the CD/DVD worklist.

Importing studies from CD/DVD

From **Patients > CD/DVD > Import** tab, import studies to the system via CD/DVD media. The CD/DVD media must be formatted as a DICOMDIR for its contents to be imported.

To import studies from a DICOMDIR CD/DVD, perform the following steps.

1. Insert the CD/DVD into the optical drive of the PACS appliance.
2. Go to **Patients > CD/DVD > Import** tab.
3. Wait for the CD/DVD to be detected by the server. When the **Status** field displays **Ready**, then the disk is compatible with the PACS appliance.
4. Select **Read Media** to read the contents of the disk. All the studies available for import display in the table.
5. Select the studies to import to the system.
 - All the selected studies are staged onto PACS appliance.
 - The job status updates to **To Be Reconciled** after the staging is completed.
 - The progress of each study will be updated as progress is made.
6. When all selected studies are imported, select **Eject Media** to physically eject the CD/DVD from the optical drive.
7. Further reconcile and manage the studies from **Studies > Reconciliation Worklist**.

Bulk Import

From **Patients > Bulk Import**, import a bulk set of patient records into the system.

Scanning volumes for import into PACS

To scan volumes for import into PACS, perform the following steps.

1. Go to **Patients > Bulk Import**. The **Scan** tab displays.
2. Insert a disk, and then select **New Scan**. The system creates one or more volumes, depending on the size of the disk, and the volume displays in the **Scans** section.
3. Select **Close**.

Importing scanned data into PACS

To import a bulk set of patient records into the system, perform the following steps.

1. Go to **Patients > Bulk Import > Import** tab.
2. Insert a disk that includes the data you want to import. The system imports the data into the system.

Studies

From **Studies**, access the following modules:

- **Study Search** - Search for existing local and remote patient study records, and access functionality for working with study records.
- **Series Search** - Search for existing local and remote patient study series records, and access functionality for working with series records.
- **Teaching File** - View and work with teaching file records that were anonymized.
- **Requests for Priors** - View current studies for which prior studies are needed to read the current studies.
- **Reconciliation Worklist** - View and reconcile studies that have been staged from outside data sources.
- **Import Store Worklist** - Manually choose on which local AE an imported study will be stored.
- **Modality Worklist** - View exams that are scheduled when the PACS system is acting as an MWL server.
- **Distributed Worklist** - View the PACS servers that are participating in an AE community.
- **Study Locks** - View all active study locks.

When **Veterinary Mode** is turned on in **Administration > System > Applications Settings > Web Administration Options** tab, then veterinary-specific fields, including **Species**, **Breed**, and **Responsible Person**, are available for creating veterinary patient records in **Patients > Create Patient**. When veterinary patient study records exist in the system, then you are able to search for them from **Studies > Study Search** and **Studies > Series Search**.

Working with veterinary study records and study series records is the same as working with human study records and human study series records.

Study Search

From **Studies > Study Search**, search for existing local and remote study records, and for the study records that display, perform any of the following tasks:

- Open patient study records to [view information related to the patient demographics](#) (patient ID, name, sex, and date of birth) and to the study, including number of series and images.
- [Attach one or more files](#) to the study record.
- [Transfer study records](#) to one or more destinations.
- [Change the status](#) of the study record.
- [Create a teaching file](#) to anonymize one or more studies for a single patient.
- [Morph the study record](#).
- [Delete the study record](#).
- [Export the study record as a .csv file](#).

Searching for patient study records

Before you are able to work with a patient study record, first search for the record from **Studies > Study Search**.

To search for a study record, perform the following steps.

1. Go to **Studies > Study Search**, and complete any of the following fields:
 - **AE Title** - Select an AE title on which to search for study records. If you select **All Local**, then options for **Change Status**, **Create Teaching File**, **Morph Study**, and **Delete** are not available.
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Patient's Name**: Enter the name of a specific patient.
 - **Sex**: Select the sex of the patient.
 - **Study Description** - Enter the description of the study.
 - **Modality** - Select a DICOM modality.
 - **Study Date** - Select the date of the study from the calendar date picker.
2. Select **Advanced**, and complete any of the additional search fields:
 - **Study Instance UID** - Enter the unique identifier of the study instance.
 - **Accession Number** - Enter the accession number assigned to the study.
 - **Original AE** - Enter the name of the original AE.
 - **Viewer Study Status** - Select the viewer status of the study.
 - **Viewer Workflow State** - Select the state of the record in the viewer workflow.
 - **Referring Physician** - Enter the name of the referring physician.
 - **Reading Physician** - Enter the name of the physician who is reading the study.
 - **Institution Name** - Enter the name of the institution where the study originated.
3. Select **Search**. The patient study records that match the criteria display, and a message confirms the number of records that match the criteria.

4. Clear the information in the Search fields by selecting **Reset**.
5. Navigate page results of patient study records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Viewing details of patient study records

From **Studies > Study Search**, search for a patient study record, and then open the record to view the DICOM attributes assigned to the study, study series, and study instances.

The steps for opening and viewing the details of patient study records that have been anonymized are the same as for viewing non-anonymized records.

To view details of a patient record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. In the row that includes the record of which you want to view details, select the **Open** folder icon. The Study Details page displays the DICOM attributes assigned to the study record.
3. From the left pane, select a study series or study instance, and the DICOM attributes for that object display, and the options for working with that object become available.
4. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Attaching files to patient study records

From **Studies > Study Search**, attach one or more files to a patient study record.

The steps for attaching files to patient study records that have been anonymized are the same as for non-anonymized records.

To attach a file to a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. In the row that includes the record to which you want to attach a file, select the **Attach** icon. The Study Attachments dialog displays.
3. In the **Document Title** field, enter the title of the file that you want to attach.
4. Select **Choose File**, select the file, and then select **Open**.
5. Select **Attach**. The file is encapsulated as a DICOM file and is attached to the study record. The file displays in the **Existing Attachments** list, and a **Delete** option displays.
6. Select **Close**. The Search page results redisplay.

Viewing attached files from patient study records

From **Studies > Study Search**, view any attached files of a study record.

To view an attached file on a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. In the row that includes the record of which you want to view an attachment, select the **Attach** icon. The Study Attachments dialog displays the list of existing attachments.
3. In the row that includes the file you want to view, select the document type icon. The document is downloaded to the location that you designate for downloaded files.

Deleting attached files from patient study records

From **Studies > Study Search**, delete attached files from a study record.

You can only delete a file from a study record if the local application entity has been configured for the delete action. Go to **Administration > DICOM > Application Entities** to determine the delete permissions for the AE.

To delete an attached file from a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. In the row that includes the record from which you want to delete an attachment, select the **Attach** icon. The Study Attachments dialog displays the list of existing attachments.

3. In the row that includes the file you want to delete, select **Delete**. The Delete dialog displays.
4. Confirm you want to delete the attachment, and then select **Yes**. A message displays confirming the file was deleted.
5. Select **Close**. The Search page results redisplay.

Manually changing status of patient study records

From **Studies > Study Search**, change the viewer study status of a study record based on the actions that have been taken on the study.

The steps for changing the status of patient study records that have been anonymized are the same as for non-anonymized records.

The default study status for pre/post fetched studies is configured in **Administration > DICOM > Study Status**.

To manually change the status of a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. Select the study for which you want to change the status, and select **Change Status**. The Change Study Status dialog displays.
3. Select the appropriate status from the following dropdown lists:
 - **Viewer Study Status**
 - **Viewer Workflow State**
4. Select **OK**. A message displays confirming the study status was successfully changed.

Creating teaching files to anonymize patient study records

From **Studies > Study Search**, create a teaching file to anonymize studies for a single patient.

View or configure anonymization settings, such as turning on anonymization mapping, from **Administration > DICOM > Tag Morphing Policies > Anonymization Settings** tab.

To anonymize a study for a single patient record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. Select the study record that you want to anonymize, and select **Create Teaching File**. The Create Teaching Files dialog displays the list of studies that will be anonymized.
3. Perform one of the following actions:
 - Manually enter the anonymous values to be used for the patient ID and patient name.
 - Select **Use Randomly Generated Identity** if you want the system to randomly generate values for patient ID and patient name.
4. Select **OK**. A message displays confirming the study has been anonymized, and the anonymized studies are available to view from **Studies > Teaching File**.

Applying tag morphing policies to patient study records

From **Studies > Study Search**, apply an existing tag morphing policy to patient study records.

View or configure tag morphing policies from **Administration > DICOM > Tag Morphing Policies**.

To apply a tag morphing policy to a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. Select the study to which you want to apply a tag morphing policy, and select **Morph Study**. The Morph Studies dialog displays the list of studies to which the policy will apply.
3. From the **Policy** dropdown list, select a tag morphing policy.
4. From the **Destination** dropdown, select the destination local AE title. The destination local AE title cannot be the AE title of the studies.
5. Select **OK**. A message displays confirming the tag morphing policy has been applied, and the process starts. The status of the process displays from the **Tasks** menu to the left of the User Profile icon.
6. From the **Tasks** menu, select the **Delete Task** icon to remove the task from the list. The Delete Task dialog displays.
7. Confirm the deletion, and select **Yes**.

Exporting patient study records to .csv files

From **Studies > Study Search**, export a study record to a .csv file.

The steps for exporting patient study records that have been anonymized are the same as for non-anonymized records.

To export a study record, perform the following steps.

1. Go to **Studies > Study Search**, and search for a patient study record. The patient study records that match the criteria display.
2. Select the study that you want to export, and select the **Export as CSV** icon. The study is downloaded as a .csv file to the location that you designate for downloaded files.

Transferring studies, series, or instances

From **Studies > Study Search > Study Details** page, transfer a study, one or more series, or one or more instances to one or more destinations, such as a local AE, remote AE, or ASTRA™ Cloud peer.

Transfer a study from **Studies > Study Search**, but transfer just a series or an instance from the Study Details page.

The steps for transferring patient study records that have been anonymized are the same as for non-anonymized records.

To transfer a study, series, or instance, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, series, or instance, and then from the **Transfer** dropdown list, select one or more locations where you want to transfer the object.
3. Select **Send**. The selected object is transferred.
4. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Viewing DICOM tags associated with study instances

From **Studies > Study Search > Study Details** page, view DICOM tags associated with a study instance.

The steps for viewing DICOM tags for study instances that have been anonymized are the same as for non-anonymized records.

To view DICOM tags associated with a study instance, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, expand the **Series** that includes the instance for which you want to view the DICOM tags, and then select the **Instance**. The DICOM attributes of that instance display, and the **View Tags** option becomes available.
3. Select **View Tags**. The View DICOM Tags dialog displays the DICOM dataset of the instance.
4. Select **Close**. The Study Details page redisplay.
5. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Viewing structured report instances

From **Studies > Study Search > Study Details** page, view a structured report instance.

Structured report instances display under study series with the modality type SR (structured report).

The steps for viewing SR instances that have been anonymized are the same as for non-anonymized records.

To view a structured report instance, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, expand the **Series** that includes the SR instance you want to view, and then select the **SR Instance**. The **View** option becomes available.
3. Select **View**. The View Structured Report dialog displays the report title, completion flag, verification flag, and the report contents.
4. Select **Close**. The Study Details page redisplay.
5. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Downloading study records

From **Studies > Study Search > Study Details** page, download a study record.

The steps for downloading patient study records that have been anonymized are the same as for non-anonymized records.

To download a study record as a .zip file, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, and then select **Download**. The Download Study dialog displays.
3. Select **OK**. The download and compression process starts. The status displays from the **Tasks** menu to the left of the User Profile icon.
4. From the **Tasks** menu, in the row that includes the study that you want to save, select **Download Study**. The .zip file is saved to your **Downloads** folder.
5. From the **Tasks** menu, select the **Delete Task** icon to remove the task from the list. The Delete Task dialog displays.
6. Confirm the deletion, and select **Yes**.
7. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Editing details of study records

From **Studies > Study Search > Study Details** page, edit the details of the study, series, or instance.

The steps for editing the details of patient study records that have been anonymized are the same as for non-anonymized records.

To edit the details of a study record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, series, or instance, and then select **Edit**. The corresponding Edit Details dialog displays the editable fields.
3. Edit information in any of the fields, and then select **OK**. A message displays confirming the changes were saved.
4. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Understanding study move operations

From **Studies > Study Search > Study Details** page, move study, series, and instance information to a patient record.

Consider the following when moving study, series, and instance information:

- When you select more than one object to move, then the objects have to be the same object type, such as all series or all instances. Selecting more than one object type at the same time will inactivate the **Move** option.
- You may select more than one instance across a series to move; however, the instances have to be of the same modality type.
- When you select a target patient record for the move, only one patient can be selected, and this patient record cannot be the original record to which the selected objects belong.
- When you select a target study for the move, the target study has to be located in the same AE where the series or instances are located, and this study cannot be the same as the original study.
- When you select a target series for the move, the modality type of the series has to be the same as the modality type of the instances you are moving, and this series cannot be the same as the original series.
- If you select more than one instance across a series for the move, the instances will be created as a single series under the target object you select.

Moving study information to patient records

From **Studies > Study Search > Study Details** page, move study information to a patient record.

The steps for moving patient study records that have been anonymized are the same as for non-anonymized records.

To move study information to a patient record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, and then select **Move**. The Move Study dialog displays.
3. Select the patient record where you want to move the study information, and then select **Next**. The Move Study summary page displays the details of the move operation.
4. Select **Finish**. A message displays confirming the selected object was moved.
5. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Moving series information to patient records

From **Studies > Study Search > Study Details** page, move study series information to a patient record.

To move study series information to a patient record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the series, and then select **Move**. The Move Series dialog displays.
3. Select the patient record where you want to move the series information, and then select **Next**.
4. Identify the study where you want to move the series by performing one of the following actions:
 - If no study was found for the patient record or you want to create a new study record, then select **Create New Study**, and a new study record will be created for the move.
 - Select an existing study.
5. Select **Next**. The Move Series summary page displays the details of the move operation.
6. Select **Finish**. A message displays confirming the series was moved.
7. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Moving study instance information to patient records

From **Studies > Study Search > Study Details** page, move study instance information to a patient record.

To move study instance information to a patient record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the instance, and then select **Move**. The Move Instances dialog displays.
3. Select the patient record where you want to move the instance information, and then select **Next**.
4. Identify the study where you want to move the instance by performing one of the following actions:
 - Select an existing study.
 - If you want to create a new study record, then select **Create New Study**, and a new study record will be created for the move.
 - If no study was found for the patient record, then a new study record will be created for the move. Select **Finish**.
5. Identify the series where you want to move the instance by performing one of the following actions:
 - If no series was found for the patient record or you want to create a new series record, then select **Create New Series**, and a new series record will be created for the move.
 - Select an existing series.
6. Select **Next**. The Move Instances summary page displays the details of the move operation.
7. Select **Finish**. A message displays confirming the instance was moved.
8. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Understanding study merge operations

From **Studies > Study Search > Study Details** page, merge a study record or one or more series records into a single patient record.

Consider the following when merging study records:

- You cannot merge an instance record into a patient record.
- When you select more than one record to merge into a single patient record, the records that you select must be of the same type; you cannot merge a study record and a series record at the same time into a patient record.
- When you select more than one series to merge into a patient record, then the series records have to be of the same modality type; selecting more than one modality type at the same time will inactivate the **Merge** option.
- When you select a target patient record for the merge, only one patient record can be selected.
- When you select a target study for the merge, the target study has to be located in the same AE where the study is located, and this study cannot be the same as the original study.
- When you select a target series for the merge, the modality type of the series has to be the same as the modality type of the instances you are merging, and this series cannot be the same as the original series.
- If you select more than one series to be merged, then the series will be created as a single series under the target series you select.

Merging study records

From **Studies > Study Search > Study Details** page, merge a study record into a single patient record.

The steps for merging patient study records that have been anonymized are the same as for non-anonymized records.

To merge a study record into a patient record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, and then select **Merge**. The Merge Study dialog displays.
3. Select the patient record where you want to merge the study information, and then select **Next**.
4. Select the study where you want to move the study record, and then select **Next**. The Merge Study summary page displays the details of the merge.

5. Confirm the merge, and then select **Finish**. A message displays confirming the study was merged.
6. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Merging study series records

From **Studies > Study Search > Study Details** page, merge one or more study series records into a single patient record.

To merge one or more study series records into a single patient record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the series, and then select **Merge**. The Merge Series dialog displays.
3. Select the patient record where you want to merge the series information, and then select **Next**.
4. Select the study where you want to move the series record, and then select **Next**.
5. Select the series where you want to move the series record, and then select **Next**. The Merge Series summary page displays the details of the merge.
6. Confirm the merge, and then select **Finish**. A message displays confirming the series was merged.
7. Select **Back to Search** to close the Study Details page and redisplay the Search page results.

Deleting study, series, or instance records

From **Studies > Study Search > Study Details** page, delete a study, series, or instance. Delete a study from **Studies > Study Search**, but delete just a series or an instance from the Study Details page.

You can only delete a study, series, or instance, from a local application entity that has been configured for the delete action. Go to **Administration > DICOM > Application Entities** to determine the delete permissions for the AE.

The steps for deleting patient study records that have been anonymized are the same as for non-anonymized records.

To delete a study, series, or instance record, perform the following steps.

1. Go to **Studies > Study Search**, and view the details of the patient study record.
2. In the left pane, select the study, one or more series, or one or more instances, and then select **Delete**. The Delete DICOM Objects dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the study, series, or instance was deleted.

Series Search

From **Studies > Series Search**, search for existing local and remote study series records, and for the study series records that display, perform any of the following tasks:

- [Transfer study series records](#) to one or more destinations.
- [Delete the study series record](#).

Searching for patient study series records

Before you are able to work with a patient study series record, first search for the record from **Studies > Series Search**.

To search for a study series record, perform the following steps.

1. Go to **Studies > Series Search**, and complete any of the following fields:
 - **AE Title** - Select an AE title on which to search for study records. If you select **All Local**, then options for **Transfer** and **Delete** are not available.
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Patient's Name**: Enter the name of a specific patient.
 - **Sex**: Select the sex of the patient.
 - **Study Description** - Enter the description of the study.
 - **Series Description** - Enter the description of the series.
 - **Modality** - Select a DICOM modality.
 - **Study Date** - Select the date of the study from the calendar date picker.
2. Select **Advanced**, and complete any of the additional search fields:
 - **Study Instance UID** - Enter the unique identifier of the study instance.
 - **Accession Number** - Enter the accession number assigned to the study.
 - **Original AE** - Enter the name of the original AE.
 - **Viewer Study Status** - Select the viewer status of the study.
 - **Priors' Status** - Select the state of any prior studies.
 - **Referring Physician** - Enter the name of the referring physician.

- **Reading Physician** - Enter the name of the physician who is reading the study.
 - **Institution Name** - Enter the name of the institution where the study originated.
 - **Series Instance UID** - Enter the unique identifier of the study series instance.
 - **Body Part Examined** - Enter the body part that was examined in the study series.
3. Select **Search**. The patient study series records that match the criteria display, and a message confirms the number of records that match the criteria.
 4. Clear the information in the Search fields by selecting **Reset**.
 5. Navigate page results of patient study series records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Transferring patient study series records

From **Studies > Series Search**, transfer a patient study series to another location.

To transfer a patient study series, perform the following steps.

1. Go to **Studies > Series Search**, and search for a patient study series record. The patient study series records that match the criteria display.
2. Select the series that you want to transfer, and from the **Transfer** dropdown list, select one or more locations where you want to transfer the study series.
3. Select **Send**. The selected object is transferred.

Deleting patient study series records

From **Studies > Series Search**, delete a patient study series record.

To delete a patient study series, perform the following steps.

1. Go to **Studies > Series Search**, and search for a patient study series record. The patient study series records that match the criteria display.
2. Select the series that you want to delete, and select **Delete**. The Delete DICOM Objects dialog displays.
3. Confirm the deletion, and then select **Yes**. A message displays confirming the series was deleted.

Teaching File

From **Studies > Teaching File**, view and work with teaching file records that are anonymized from **Studies > Study Search** and based on the system default teaching policies that are configured from **Administration > DICOM > Teaching File Policy**.

Searching for teaching file patient study records

Before you are able to work with an anonymized patient study record, first search for the record from **Studies > Teaching File**.

To search for a teaching file patient study record, perform the following steps.

1. Go to **Studies > Teaching File**, and complete any of the following fields:
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Patient's Name**: Enter the name of a specific patient.
 - **Sex**: Select the sex of the patient.
 - **Study Description** - Enter the description of the study.
 - **Modality** - Select a DICOM modality.
 - **Study Date** - Select the date of the study from the calendar date picker.
2. Select **Search**. The patient study records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Clear the information in the Search fields by selecting **Reset**.
4. Navigate page results of patient study records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Working with anonymized patient study records

From **Studies > Teaching File**, view and work with teaching file records. The steps for working with patient study records that have been anonymized in **Studies > Study Search** are the same as for non-anonymized records. Refer to the following procedures:

- [Viewing details of patient study records](#)

- [Attaching files to patient study records](#)
- [Manually changing status of patient study records](#)
- [Exporting patient study records to .csv files](#)
- [Transferring studies, series, or instances](#)
- [Viewing DICOM tags associated with study instances](#)
- [Viewing structured report instances](#)
- [Downloading study records](#)
- [Editing details of study records](#)
- [Moving study information to patient records](#)
- [Merging study records](#)

Requests for Priors

Studies > Requests for Priors displays current patient study records for which prior studies may be needed to read the current study as a whole or to make an addendum to a current study that was read without any or all prior studies.

The current studies in the Requests for Priors list have any of the following viewer workflow states:

- **Hold for Priors** - Indicates that a radiologist has chosen to delay reading the study because prior studies that are necessary for reading are unavailable, or no prior studies are available at all. The hold period may be from 1 to 30 days and is configured from **Administration > DICOM > Study Status**.
- **Hold Period Expired** - Indicates that the configured hold period has elapsed for the current study and that prior studies for the current study could not be retrieved in time. The current study must be read as soon as possible.
- **Priors Requested** - Indicates that a radiologist desires that a particular set of prior records be available for the current read of the study. Some prior studies may be available on the server, but not all are available, or studies may need to be retrieved from an external study.

For a complete list of viewer workflow states and their descriptions, refer to the *Advanced Viewer User Manual*.

Viewing patient study records listed in Requests for Priors

From **Studies > Requests for Priors**, view a list of current studies that have a viewer workflow state of Hold for Priors, Hold Period Expired, or Priors Requested. The following options are suggested for working with studies that display in this list:

- Search for prior studies for the current study, and store them via import and reconciliation. When the priors are imported and reconciled, then the request for priors will disappear automatically.
- Cancel the request for priors by selecting **Cancel** next to the study in the list. The study record will be removed from the list, and the viewer workflow status will be changed to Canceled. If the local AE where the current study resides is configured with a Peer for Priors Exchange workflow, then the status will be sent to the peer.

To manually change the viewer study status and viewer workflow state of a patient study record, go to **Studies > Study Search**.

Reconciliation Worklist

When importing studies from outside data sources, such as CD/DVD or from ASTRA™ Cloud peers, some of the patient demographics data, such as patient name, birth date, and sex, may not exactly match demographics for the patient ID that is already found on the PACS server. If the demographic data is not handled properly, then multiple records for the same physical patient may be imported into the PACS. However, staging records to the Reconciliation Worklist allows you to reconcile differences in patient demographics data before storing them in the PACS.

From **Studies > Reconciliation Worklist**, view and reconcile studies that have been staged from outside data sources to the Reconciliation Worklist. Studies imported from CD/DVD using a PACS image viewer or received from ASTRA™ Cloud can also be imported through the Reconciliation Worklist.

- Import reconciliation settings are configured from **Administration > DICOM > Import Service > Settings** tab.
- Conflict evaluation parameters are configured from **Administration > Patient > Quality Control**.

Reconciling patient demographics data in imported studies

From **Studies > Reconciliation Worklist**, reconcile patient demographics data, such as patient ID, patient name, birth date, and sex, in studies that have been staged to the Reconciliation Worklist from outside data sources. Outside sources may include, but not be limited to, CD/DVD using a PACS image viewer or ASTRA Cloud peers.

To reconcile patient demographics data in imported studies staged to the Reconciliation Worklist, perform the following steps.

1. Go to **Studies > Reconciliation Worklist**. Studies that have been staged to the Reconciliation Worklist display.
2. Filter studies as needed by entering data in any of the Search fields and selecting **Search**.
3. Select one or more studies for which you want to reconcile patient demographics data, and then select **Reconcile**. The Import Reconciliation dialog displays the patient demographics that are used in one or more of the imported studies.
4. For each patient record to reconcile, select one of the following options:
 - Use the patient demographics from the imported study.
 - Select one of the patients suggested by the system. Patient demographics that are similar among the patient records are highlighted in green text.
 - Search for an existing patient to use.
 - Create a new patient record.
5. Select one of the following options:
 - Select **Next** to reconcile another patient record. The Import Reconciliation dialog displays the next patient record to reconcile.
 - Select **Finish** to complete the reconciliation process. The corresponding study for each patient is saved with the demographics data that you specified and is automatically stored on the destination AE that was configured from **Administration > DICOM > Import Service > Settings** tab.

Additional system operations performed on imported studies

The PACS system is configured with default study workflows that can be used to process studies, based on the availability of prior studies. When the viewer workflow and viewer workflow states are being used, then the system performs additional operations on the study to be imported.

When studies that are about to be imported are priors and a current study that is already stored has one of the following workflow states, then the system changes the status of the study as follows:

- Hold for Priors: The system changes the status of the current study to Priors Available.
- Hold Period Expired: The system changes the status of the current study to Priors Available.
- Priors Requested: The system changes the status of the current study to Priors Requested, Addendum Check.
- Completed: The system changes the status of the current study to Addendum Check.

If the destination local AE for the imported studies is configured with a peer for priors exchange workflow, then the system transmits the study status to the peer.

If the import destination is not configured, then after the reconciliation process, the system stages the studies to the Import Store Worklist. From the Import Store Worklist, manually choose on which local AE the imported study will be stored.

Deleting studies from Reconciliation Worklist

To permanently delete studies from the Reconciliation Worklist, perform the following steps.

1. Go to **Studies > Reconciliation Worklist**. Studies that have been staged to the Reconciliation Worklist display.
2. Select one or more studies that you want to delete, and then select **Delete**. The Delete Reconciliation Worklist Order dialog displays.
3. Confirm the deletion, and then select **Yes**. The selected studies are permanently deleted.

Import Store Worklist

When an import destination has not been configured, then all imported studies that have already gone through the reconciliation process are automatically staged in **Studies > Import Store Worklist**. From the Import Store Worklist, manually choose on which local AE the imported study will be stored.

The Import Service may also be configured to bypass the reconciliation process for studies imported from specific sources. In these cases, imported studies are directly staged to the Import Store Worklist instead of the Reconciliation Worklist. Import service policies and settings are configured from **Administration > DICOM > Import Service**.

Manually storing studies to local AEs

From **Studies > Import Store Worklist**, manually choose on which local AE imported studies will be stored.

To manually store studies into a local AE, perform the following steps.

1. Go to **Studies > Import Store Worklist**. Studies that have been staged to the Import Store Worklist display.
2. Filter studies as needed by entering data in any of the Search fields and selecting **Search**.
3. Select one or more studies, select **Store**, and from the dropdown list, select the local AE where to store the study selected.

4. Select **Store**. The study is stored in the local AE and is automatically removed from the Import Store Worklist. If a failure occurs, then the job remains on the Import Store Worklist with the status Failed.

Deleting studies from Import Store Worklist

To permanently delete studies in the Import Store Worklist, perform the following steps.

1. Go to **Studies > Import Store Worklist**. Studies that have been staged to the Import Store Worklist display.
2. Select one or more studies that you want to delete, and then select **Delete**. The Delete Import Store Worklist dialog displays.
3. Confirm the deletion, and then select **Yes**. The selected studies are permanently deleted.

Modality Worklist

The DICOM[®] Modality Worklist (MWL) is a standard that allows information to be exchanged between medical imaging devices and clinical applications. For example, the MWL service identifies patients who are scheduled for a study, and the workflow engine retrieves this patient schedule on a regular basis and applies a range of filters. These filters select or remove patient records according to site-specific configuration settings. When modalities are configured to query the MWL to automate the data entry process, then unintentional errors that may occur during manual data entry may be avoided.

The PACS system can act as an MWL server, an MWL client, or both.

- When acting as a server, the PACS system will receive C-FIND requests and respond based on the given criteria.
- When acting as a client, the PACS system can send C-FIND requests to a remote MWL and perform the appropriate actions, such as prefetching matching priors, based on the response.

From **Studies > Modality Worklist**, view procedures that are scheduled when the PACS system is acting as an MWL server and when the system is acting as an MWL client.

Viewing procedures on Local Modality Worklist

From **Studies > Modality Worklist**, view procedures that are scheduled when the PACS system is acting as a Modality Worklist (MWL) server.

Local modality worklist entries may be built via the following sources:

- HL7 service upon receiving ORM or SIU messages
- PACS appliance RIS application

If the PACS system is not acting as an MWL server, then the Modality Worklist will be empty.

To view procedures on the local MWL, perform the following steps.

1. Go to **Studies > Modality Worklist > Local** tab. Procedures scheduled on the local MWL that have the status Pending, Scheduled, In Progress, Completed, and Canceled display.
2. Filter studies as needed by entering data in any of the Search fields and selecting **Search**.

Rescheduling procedures on Local Modality Worklist

From **Studies > Modality Worklist > Local** tab, reschedule procedures that are on the local MWL.

To reschedule procedures on the local MWL, perform the following steps.

1. Go to **Studies > Modality Worklist > Local** tab. Procedures scheduled on the local MWL that have the status Pending, Scheduled, In Progress, Completed, and Canceled display.
2. Select one or more procedure records, and then select **Reschedule**. The Reschedule Modality Worklist Orders dialog displays.
3. Complete the **Date** and **Time** fields, and then select **OK**. The changes are saved.

Deleting procedure records from Local Modality Worklist

To permanently delete procedure records from the Local MWL, perform the following steps.

1. Go to **Studies > Modality Worklist > Local** tab. Procedures scheduled on the local MWL that have the status Pending, Scheduled, In Progress, Completed, and Canceled display.

2. Select one or more procedure records that you want to delete, and then select **Delete**. The Delete Modality Worklist Order dialog displays.
3. Confirm the deletion, and then select **Yes**. The selected study procedure records are permanently deleted.

Viewing procedures on Remote Modality Worklist

From **Studies > Modality Worklist > Remote** tab, view procedures that are scheduled when the PACS system is acting as an MWL client. You cannot modify the procedure records that display in the remote Modality Worklist; the records are read-only.

Remote MWL servers must be registered on the PACS system as remote AEs from **Administration > DICOM > Application Entities > Remote** tab.

To view procedures on the remote MWL, perform the following steps.

1. Go to **Studies > Modality Worklist > Remote** tab. Procedures scheduled on the local MWL that have the status Pending, Scheduled, In Progress, Completed, and Canceled display.
2. Filter studies as needed by entering data in any of the Search fields and selecting **Search**.

Distributed Worklist

From **Studies > Distributed Worklist**, view the PACS servers that are participating in an AE community, and view a list of current (unread) studies that are located on the local AEs that have been added to the existing AE community.

If an AE community has not been created, then the Distributed Worklist will be empty.

To create an AE community, go to **Administration > System > Distributed Worklist > Membership** tab.

Transferring studies to AEs in an AE community

From **Studies > Distributed Worklist**, send current studies to AEs in your AE community. If an AE community has not been created, then the Distributed Worklist will be empty.

If you want to transfer a study to a location, such as a remote AE or an ASTRA[™] peer, that is not part of an AE community, go to **Studies > Study Search**.

To transfer a study to an AE in your AE community, perform the following steps.

1. Go to **Studies > Distributed Worklist**. The PACS servers that are part of the AE community display.
2. Expand the list of studies to find the study that you want to transfer to an AE in the community.
3. Select the row of the study, and from the **Transfer** dropdown list, select the AE to which to transfer the study, and then select **Send**.

View the studies from an image viewer.

Study Locks

From **Studies > Study Locks**, view all study records that have been automatically locked by the system. Locking studies prevents the same study from being accessed and updated by different applications and/or users at the same time.

Manually releasing locked study records

From **Studies > Study Locks**, manually release a locked study. Select **Refresh** to refresh the list.

To manually release a locked study record, perform the following steps.

1. Go to **Studies > Study Locks**. A list of locked study records display.
2. In the row that includes the locked study that you want to release, select **Delete**. The study record is unlocked. The process of deleting the study lock releases the lock; the process does not delete the study record.
3. Release all study locks by selecting **Delete All**.

Transfers

From **Transfers**, access the following modules:

- **Routing Worklist** - View and manage the send and move routing jobs.
- **Pre/Post Fetching Worklist** - View and manage prefetching and postfetching jobs.
- **Backup Catalog** - View study catalog records and system catalog records.
- **Backup Worklist** - View and manage archive, backup, and restore jobs.
- **HL7 Worklist** - View and manage HL7 messages.
- **ASTRA Worklist** - View and manage ASTRA™ Cloud jobs.

Routing Worklist

From **Transfers > Routing Worklist**, view and manage DICOM® object transfers (hereafter referred to as routing jobs). Routing jobs that display in the Routing Worklist were sent or moved manually via the **Studies > Study Search** or sent automatically via routing policies configured in **Administration > DICOM > Routing Policies**.

The routing jobs in the Routing Worklist may be one of the following job types:

- Send jobs: Sending studies to remote application entities (AEs)
- Move jobs: Moving studies from one AE to another AE

The worklist manager runs in the background and processes routing jobs according to the schedule configured in **Administration > DICOM > Routing Policies**.

Searching for routing jobs in Routing Worklist

Before working with a send or move routing job, first search for a job from **Transfers > Routing Worklist**.

To search for a routing job in Routing Worklist, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and complete any of the following fields:
 - **From**: Select the source AE title.
 - **To**: Select the destination AE title.
 - **Status**: Select the status of the job.
 - **Policy Type**: Select the type of routing policy.
 - **Policy ID**: Enter one or more IDs, separated by a comma, of the policy that created the routing job.
 - **Job ID**: Enter one or more IDs, separated by a comma, of the send or move job.
 - **Error Message**: Enter error message text to filter for jobs that failed and displayed an error message.
 - **Scheduled Date**: Select the date of the job from the calendar date picker.
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Patient's Name**: Enter the name of a specific patient.
 - **Accession Number**: Enter the accession number.
 - **Study Instance UID**: Enter the UID of the study instance.
 - **Series Instance UID**: Enter the UID of the series instance.
 - **Modality**: Select a modality.
 - **Description**: Enter a brief description of the routing job.
 - **Study Date**: Select the date of the study from the calendar date picker.
2. Select **Search**. The routing jobs that match the criteria display, and a message confirms the number of records that match the criteria.
3. Clear the information in the Search fields by selecting **Reset**.
4. Navigate page results of routing jobs by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Sort results in ascending or descending order by a criteria, such as **Status** or **Scheduled Date**, by selecting the option from the **Sort By** dropdown list.

Viewing details of jobs in Routing Worklist

From **Transfers > Routing Worklist**, view the details of a job in the Routing Worklist.

To view the details of a job, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and search for a routing job. The routing jobs that match the criteria display.

2. In the row that includes the job for which you want to view the details, select the **View Details** icon. The Job dialog displays job information and timestamped messages.
3. Select **Close**. The search results redisplay.

Viewing transaction records of jobs in Routing Worklist

From **Transfers > Routing Worklist**, view transaction records of jobs in Routing Worklist.

Only jobs that send studies to remote AEs with the storage commitment option turned on will have transaction records.

To view the transaction record of a job, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and search for a routing job. The routing jobs that match the criteria display.
2. In the row that includes the job for which you want to view the transaction record, select the **Storage Commitment Record** icon. The Storage Commitment Record dialog displays.
3. Select **Close**. The search results redisplay.

Retrying failed jobs in Routing Worklist

To retry a failed job, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and search for routing jobs with a status of Failed. The routing jobs that match the criteria display.
2. In the row that includes the failed job you want to retry, select the **Retry Now** icon. The system performs the job action, and the status displays.

Rescheduling jobs in Routing Worklist

To reschedule a job in the Routing Worklist, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and search for a routing job. The routing jobs that match the criteria display.
2. Select one or more jobs that you want to reschedule, and then select **Reschedule**. The Reschedule Worklist Jobs dialog displays.
3. Complete the **Date** and **Time** fields, and then select **OK**. A message displays confirming the worklist job is rescheduled.

Deleting jobs in Routing Worklist

To delete a job from the Routing Worklist, perform the following steps.

1. Go to **Transfers > Routing Worklist**, and search for a routing job. The routing jobs that match the criteria display.
2. Select one or more jobs that you want to delete, and then select **Delete**. The Delete Worklist Jobs dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the worklist job has been deleted.

Pre/Post Fetching Worklist

From **Transfers > Pre/Post Fetching Worklist**, view and manage prefetching and postfetching jobs. Prefetching and postfetching jobs are generated to automatically transfer prior studies to the appropriate destinations based on the configured routing policies.

- Prefetching jobs are created when a prefetching rule is triggered by scheduled exams on the modality worklist (MWL). These jobs are configured in **Administration > DICOM > Prefetching Policies**.
- Postfetching jobs are created when a postfetching rule is triggered by an incoming study. These jobs are configured in **Administration > DICOM > Postfetching Policies**.

The worklist manager runs in the background and processes prefetching and postfetching jobs according to the schedule configured in **Administration > DICOM > Prefetching Policies** or **Postfetching Policies**. Jobs are assigned the following statuses as they move through the routing process.

- Pending: Status while jobs await processing.
- In Progress: Status while jobs are being processed.
- Completed: Status when a job is processed by the system successfully, which means the appropriate number of routing jobs were created to retrieve prior studies.
- Pending *n* Retries: Status when a job fails and will be retried at a later time. *n* designates the number of times the job has been retried by the system.
- Failed: Status when a job fails and the configured maximum number of retries has been reached.

Searching for prefetching and postfetching jobs in Pre/Post Fetching Worklist

Before working with prefetching and postfetching jobs, first search for a job from **Transfers > Pre/Post Fetching Worklist**.

To search for a prefetching or postfetching job in Pre/Post Fetching Worklist, perform the following steps.

1. Go to **Transfers > Pre/Post Fetching Worklist**, and complete any of the following fields:
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Patient's Name**: Enter the name of a specific patient.
 - **Status**: Select the status of the job.
2. Select **Search**. The jobs that match the criteria display, and a message confirms the number of records that match the criteria.
3. Navigate page results of prefetching and postfetching jobs by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending order by selecting a column header.

Viewing fetching triggered jobs in Pre/Post Fetching Worklist

From **Transfers > Pre/Post Fetching Worklist**, view a list of routing jobs that were triggered by the prefetching or postfetching job that you select.

Manage the prefetching or postfetching job from **Transfers > Routing Worklist**. The ID for the prefetching or postfetching job does not match the job ID that is assigned in the Routing Worklist.

To view fetching triggered jobs in Pre/Post Fetching Worklist, perform the following steps.

1. Go to **Transfers > Pre/Post Fetching Worklist**, and search for a prefetching or postfetching job. The jobs that match the criteria display.
2. In the row that includes the prefetching or postfetching job for which you want to view the fetching list, select the **Magnifying Glass** icon. The Fetching Triggered Jobs dialog displays the routing jobs that were triggered by the prefetching or postfetching job that you selected.
3. At the bottom of the dialog select **OK** to close the list. If the fetching list is long, then you may have to scroll to the bottom of the dialog to see the **OK** option. The search results redisplay.

Rescheduling jobs in Pre/Post Fetching Worklist

To reschedule a prefetching or postfetching job in the Pre/Post Fetching Worklist, perform the following steps.

1. Go to **Transfers > Pre/Post Fetching Worklist**, and search for a prefetching or postfetching job. The jobs that match the criteria display.
2. Select one or more jobs that you want to reschedule, and then select **Reschedule**. The Reschedule Worklist Jobs dialog displays.
3. Complete the **Date** and **Time** fields, and then select **OK**. A message displays confirming the worklist job is rescheduled.

Deleting jobs in Pre/Post Fetching Worklist

To delete a prefetching or postfetching job from the Pre/Post Fetching Worklist, perform the following steps.

1. Go to **Transfers > Pre/Post Fetching Worklist**, and search for a prefetching or postfetching job. The jobs that match the criteria display.
2. Select one or more prefetching or postfetching jobs that you want to delete, and then select **Delete**. The Delete Worklist Jobs dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the worklist job has been deleted.

Backup Catalog

From **Transfers > Backup Catalog**, view study catalog records and system catalog records for objects, such as attachments and backup databases, that have been exported to a storage destination.

Searching for study catalog records

To search for study catalog records, perform the following steps.

1. Go to **Transfers > Backup Catalog > Study Catalog** tab, and complete any of the following fields:
 - **AE Title**: Select the AE title on which the original study is stored.

- **Patient ID:** Enter the primary identification number for the patient.
 - **Patient's Name:** Enter the name of a specific patient.
 - **Study Date:** Select the date of the study from the calendar date picker, or select a preset date range.
 - **Study Instance UID:** Enter the unique identifier of the study.
 - **Storage Destination:** Select the destination where the study is stored.
2. Select **Search**. The study catalog records that match the criteria display, and a message confirms the number of records that match the criteria. The following information displays for each record to help locate the record when it needs to be restored.
 - **ID:** Displays the unique identifier of the record.
 - **Storage Destination:** Identifies the storage destination (SD) where this record is located.
 - **Patient ID:** Identifies the the primary identification number for the patient of the study record.
 - **Patient's Name:** Identifies the name of a specific patient of the study record.
 - **AE Title:** Identifies the AE title where the study was located before being exported to the SD.
 - **Study Date:** Identifies the date of the study.
 - **Study Description:** Displays a brief description of the study.
 - **Last Modified Date:** Identifies the time when the study was last modified.
 - **Completed Time:** Identifies the time when the study record was recorded on the SD.
 - **Expiration Time:** Identifies the time when the study record expires; the default expiration time is set to 15 years.
 - **Storage Detail:** Identifies storage-specific information to locate the study object.
 - **Files:** Displays the number of image files stored on the SD for this study object.
 3. Navigate page results of records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending order by selecting a column header.

Restoring study catalog records

From **Transfers > Backup Catalog > Study Catalog** tab, restore study records from the storage destination to the PACS system.

To restore a study catalog record, perform the following steps.

1. Go to **Transfers > Backup Catalog**, and search for a study catalog record. The study catalog records that match the criteria display, and a message confirms the number of records that match the criteria.
2. Select one or more study records, and then select **Restore**. A single restore job is added to the Backup Worklist for the study records that you selected.

Searching for system catalog records

To search for system catalog records, perform the following steps.

1. Go to **Transfers > Backup Catalog > System Catalog** tab, and complete the following fields:
 - **Storage Destination:** Select the SD on which the system data object is stored.
 - **Type:** Select the type of the system data object that is stored on the SD.
2. Select **Search**. The system catalog records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Navigate page results of records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending order by selecting a column header.

Backup Worklist

From **Transfers > Backup Worklist**, view and manage archive, backup, and restore jobs. Jobs that display in the Backup Worklist are generated based on Backup Service policies that are configured and turned on in **Administration > Data Management > Backup Service**.

Examples of data objects that may be stored may include, but are not limited to, attachments, backup-related databases, and configuration files.

You must have a license to use the Backup Worklist feature. Contact your sales representative if you want to purchase a Backup Worklist license for your PACS system.

Searching for backup job records in Backup Worklist

To search for a backup job record in Backup Worklist, perform the following steps.

1. Go to **Transfers > Backup Worklist**, and complete the following fields:
 - **From**: Select the source storage destination.
 - **To**: Select the destination storage destination.
 - **Type**: Select the type of the data object that was stored. If you select the Study Type, then fields for **Patient ID** and **Patient's Name** also display for data entry.
 - **Status**: Select the status of the backup job.
2. Select **Search**. The backup job records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Navigate page results of backup jobs by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending order by selecting a column header.

Retrying pending or failed jobs in Backup Worklist

To retry pending or failed jobs in Backup Worklist, perform the following steps.

1. Go to **Transfers > Backup Worklist**, and in the **Status** field, select **Failed** or **Pending**.
2. Select **Search**. The failed or pending backup job records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Select one or more backup jobs that you want to retry, and then select **Retry**. The system performs the job action, and the status displays.

Deleting failed backup jobs from Backup Worklist

To delete backup jobs from Backup Worklist that have the status Failed, perform the following steps.

1. Go to **Transfers > Backup Worklist**, and in the **Status** field, select **Failed**.
2. Select **Search**. The failed backup job records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Select one or more failed backup jobs that you want to delete, and then select **Delete**. The Delete Worklist Jobs dialog displays.
4. Confirm the deletion, and select **Yes**. A message displays confirming the worklist job has been deleted.

HL7 Worklist

From **Transfers > HL7 Worklist**, view both inbound and outbound HL7 messages that have been received, sent, or are pending to be sent by the HL7 Service configured in **Administration > HL7 > HL7 Service**. HL7 peers and message triggers are configured in **Administration > HL7 > HL7 Peers**.

Searching for HL7 messages in HL7 Worklist

To search for HL7 messages in HL7 Worklist, perform the following steps.

1. Go to **Transfers > HL7 Worklist**, and select the **Inbound** tab or the **Outbound** tab.
2. Complete the following fields:
 - **Patient ID**: Enter the primary identification number for the patient in the HL7 message.
 - **Patient's Name**: Enter the name of the specific patient in the HL7 message.
 - **Accession Number**: Enter the number of the accession record.
 - **Date**: From the calendar date picker, select the date when the HL7 message was received if inbound or when the HL7 message was sent if outbound.
 - **Peer**: Select the HL7 peer from which the message was received if inbound or to which HL7 peer the message was sent if outbound.
 - **Message Type**: Select the type of message that was sent or received.
 - **Trigger Event**: Select the trigger event of the HL7 message. Options to select are based on your Backup Worklist selection in the **Message Type** field; if you select All, then you cannot select a trigger event.
 - **Status**: Select the status of the HL7 message.
3. Select **Search**. The HL7 messages that match the criteria display, and a message confirms the number of records that match the criteria.
4. Navigate page results of HL7 messages by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Viewing details of HL7 messages in HL7 Worklist

To view details of inbound or outbound HL7 messages in HL7 Worklist, perform the following steps.

1. Go to **Transfers > HL7 Worklist**, and search for an HL7 message from the **Inbound** tab or the **Outbound** tab. The HL7 messages that match the criteria display, and a message confirms the number of records that match the criteria.
2. In the row that includes the HL7 message of which you want to view the details, select the **Open** folder icon. The HL7 message dialog displays each segment of the message. Expand each segment to view the contents of each field.
3. Select **Close**. The search results redisplay.

Retrying pending or failed HL7 messages in HL7 Worklist

To retry pending or failed inbound or outbound HL7 messages in HL7 Worklist, perform the following steps.

1. Go to **Transfers > HL7 Worklist**, and select the **Inbound** tab or the **Outbound** tab.
2. In the **Status** field, select **Failed** or **Pending**, and then select **Search**. The failed or pending HL7 message records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Select one or more HL7 messages that you want to retry, and then select **Retry**. The system performs the HL7 message action, and the status displays.

Deleting HL7 messages from HL7 Worklist

Completed HL7 message jobs are automatically deleted from the HL7 Worklist after the period of time configured from **Administration > HL7 > HL7 Service > Worklist** tab.

To manually delete HL7 messages from HL7 Worklist, perform the following steps.

1. Go to **Transfers > HL7 Worklist**, and search for an HL7 message from the **Inbound** tab or the **Outbound** tab. The HL7 messages that match the criteria display, and a message confirms the number of records that match the criteria.
2. Select one or more HL7 messages that you want to delete, and then select **Delete**. The Delete HL7 Worklist Jobs dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the worklist job has been deleted.

Exporting HL7 messages from HL7 Worklist

To export HL7 messages from HL7 Worklist, perform the following steps.

1. Go to **Transfers > HL7 Worklist**, and search for an HL7 message from the **Inbound** tab or the **Outbound** tab. The HL7 messages that match the criteria display, and a message confirms the number of records that match the criteria.
2. Select one or more HL7 messages that you want to export, and then select **Export**.
 - If you select an inbound message, the Export Inbound HL7 Message dialog displays.
 - Select which inbound message to export, or select **All**, and then select **OK**.
 - The HL7 file is downloaded to the location that you designate for downloaded files.

ASTRA Worklist

From **Transfers > ASTRA Worklist**, view and manage ASTRA™ Cloud jobs that have been configured in **Administration > ASTRA > ASTRA Peers**.

You must register the PACS appliance with ASTRA™ Cloud to access the ASTRA Worklist. Go to **Administration > ASTRA > ASTRA Service > Registration** tab.

Searching for ASTRA Cloud jobs in HL7 Worklist

To search for ASTRA Cloud jobs in ASTRA Worklist, perform the following steps.

1. Go to **Transfers > ASTRA Worklist**, and complete the following fields:
 - **Status**: Select the status of the ASTRA Cloud job.
 - **Type**: Select the type of ASTRA Cloud message.
 - **Action**: Select the action that the ASTRA Cloud peer is performing.
2. Select **Search**. The ASTRA Cloud job records that match the criteria display, and a message confirms the number of records that match the criteria.
3. Navigate page results of ASTRA Cloud job records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.

Viewing details of ASTRA Cloud jobs in ASTRA Worklist

To view details of ASTRA Cloud jobs in ASTRA Worklist, perform the following steps.

1. Go to **Transfers > ASTRA Worklist**, and search for an ASTRA Cloud job. The ASTRA Cloud jobs that match the criteria display, and a message confirms the number of records that match the criteria.
2. In the row that includes the ASTRA Cloud job of which you want to view the details, select the **Open** folder icon. The ASTRA dialog displays the job details.

Retrying ASTRA Cloud jobs in ASTRA Worklist

To retry ASTRA Cloud jobs in ASTRA Worklist, perform the following steps.

1. Go to **Transfers > ASTRA Worklist**, and search for an ASTRA Cloud job. The ASTRA Cloud jobs that match the criteria display, and a message confirms the number of records that match the criteria.
2. Select one or more ASTRA Cloud jobs that you want to retry, and then select **Retry**. The system performs the ASTRA Cloud job action, and the status displays.

Deleting ASTRA Cloud jobs from ASTRA Worklist

To manually delete ASTRA Cloud jobs from ASTRA Worklist, perform the following steps.

1. Go to **Transfers > ASTRA Worklist**, and search for an ASTRA Cloud job. The ASTRA Cloud jobs that match the criteria display, and a message confirms the number of records that match the criteria.
2. Select one or more ASTRA Cloud jobs that you want to delete, and then select **Delete**. The Delete Worklist Jobs dialog displays.
3. Confirm the deletion, and select **Yes**. A message displays confirming the worklist job has been deleted.

Reports

From **Reports**, access the following modules:

- **Statistical Reports** - View system usage reports.
- **Audit Trail** - View messages of audited system events.
- **XDS Registry Objects** - View metadata for all submission sets, folders, and documents registered with the XDS Registry.
- **XDS Repository Objects** - View documents currently stored on the XDS Repository.

Statistical Reports

From **Reports > Statistical Reports** view system-generated reports based on current data in the system. The following reports are available in the system:

- **General Statistics**: Provides statistics related to the number of studies, series, and images in each local AE title and the number for all AEs combined.
- **Modality Statistics**: Provides statistics related to the total number of images per modality type in each local AE.
- **AE Storage Usage**: Provides the study storage usage information for each local AE.
- **Studies per Month**: Provides statistics related to the number of studies that were generated each month on each local AE based on the study date.

Generating statistical reports

1. Go to **Reports > Statistical Reports**.
2. From the dropdown list, select the name of the report you want to view.
3. Select one of the following options:
 - **Show Report**: Display the report information that was generated at midnight. The timestamp of the report designates the time when the report was generated.
 - **Generate Report**: Display the report information that is generated in real time. This report may take some time to complete. The report is generated based on the existing data on the system and the selection that you made.

Audit Trail

From **Reports > Audit Trail**, view messages of audited system events. Each audit message corresponds to one audited event.

Audit messages may be used for surveillance, troubleshooting, disclosure logs, or for forensic investigations mandated after a security breach or any kind of policy violation has been detected.

Viewing audit trail messages

To view audit trail messages, perform the following steps.

1. Go to **Reports > Audit Trail**, and complete any of the following fields:
 - **Event Date Time Range**: Select a date time range for the event search.
 - **Refined Event Date Range**: Select the date from the calendar date picker.
 - **AE Title**: Select a local or remote AE title.
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Study Instance UID**: Enter the study instance UID of a specific study.
 - **Event ID**: Select the specific audited event.
 - **Event ID Type**: Select the category of event.
2. Select **Advanced**, and complete any of the following fields:
 - **Participant**: Select the active participant for the audit event.
 - **Application**: Select the application involved for the audit event. This option is only available when you select Application in the **Participant** field.
 - **Real Name**: Enter the registered real name of the user who is involved in the audit event. This option is only available when you select User in the **Participant** field.
 - **Sign-In Name**: The registered sign-in name of the user who is involved in the audit event. This option is only available when you select User in the **Participant** field.
 - **Outcome**: Select the outcome of the audit event.
 - **Action**: Select the action type of the audit event.
3. Select **Search**. The audit event records that match the criteria display, and a message confirms the number of records that match the criteria.
4. Navigate page results of audit event records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.

- Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending date by selecting the arrow next to the **Date** column header.
5. In the row that includes the audit event of which you want to view the details, select the **Open** folder icon. The View Audit Message dialog displays the XML version of the audit message.
 6. Select **Close**. The search results redisplay.

XDS Registry Objects

From **Reports > XDS Registry Objects**, view metadata for all submission sets, folders, and documents registered with the XDS Registry, if your system is acting as one.

Viewing objects registered with XDS Registry

To view objects registered with XDS Registry, perform the following steps.

1. Go to **Reports > XDS Registry Objects**, and select the **Submission Sets** tab, the **Folders** tab, or the **Documents** tab.
2. Complete any of the following fields:
 - **Unique ID**: Enter the unique identifier for the submission set, folder, or document.
 - **Entry UUID**: Enter the entry UUID for the submission set, folder, or document.
 - **Patient ID**: Enter the primary identification number for the patient.
 - **Title**: Enter the title of the submission set, folder, or document.
 - **Source ID**: Enter the unique identifier of the XDS source that registered the submission set. This field only displays on the **Submission Sets** tab.
 - **Repository ID**: Enter the unique identifier of the XDS repository where documents are stored. This field only displays on the **Documents** tab.
3. Select **Search**. The XDS Registry records that match the criteria display, and a message confirms the number of records that match the criteria.
4. Navigate page results of records by performing any of the following actions:
 - Go to a specific page of results by selecting a page number from the **Page** dropdown list.
 - Go to the next page or previous page of results by selecting the respective arrow next to the **Page** dropdown list.
 - Filter results by ascending or descending unique ID by selecting the arrow next to the **Unique ID** column header.
5. In the row that includes the XDS Registry records of which you want to view the details, select the **Open** folder icon. The XDS Registry dialog displays the metadata of the object selected.

XDS Repository Objects

From **Reports > XDS Repository Objects**, view documents currently stored on the XDS Repository, if your system is acting as one.

Viewing objects stored on XDS Repository

1. Go to **Reports > XDS Registry Objects**.
2. In the **Unique ID** field, enter the unique identifier for the document, and select **Search**. The XDS document records that match your criteria display, and a message confirms the number of records that match the criteria.
3. Save a copy of the document to your computer by selecting the **Download** icon in the row of the document record.

Help & Troubleshooting

From **Help & Troubleshooting**, access the following modules:

- **Remote Assistance** - View contact information for the technical support center.
- **Diagnostic Tools** - Capture and collect relevant system data used by technical support to troubleshoot issues.
- **Network Tools** - Perform some simple network tests, and view a list of concurrent network connections.
- **Network Activity** - View network activity.
- **Server Logs** - View server logs.
- **Documents** - View help documents.

Remote Assistance

From **Help & Troubleshooting > Remote Assistance**, view contact information for technical support center.

Contacting Technical Support

To contact technical support, perform the following steps.

1. Go to **Help & Troubleshooting > Remote Assistance > Contact Information** tab.
2. Contact technical support by sending an email message to support@candelis.com.
3. Contact US technical support directly via phone by dialing +1.800.800.8600.
4. Contact international technical support directly via phone by dialing +1.949.852.1000.

Connecting to the Technical Support Center

After contacting technical support, you may be asked to connect the PACS appliance server to the Technical Support Center (TSC) so that the engineers may remotely access your PACS appliance. This can be done via the PACS appliance **Help & Troubleshooting > Remote Assistance > Technical Support Center** tab.

To open a Technical Support Center (TSC) connection, perform the following steps.

1. Go to **Help & Troubleshooting > Remote Assistance > Technical Support Center** tab, and complete the following fields:
 - **Host Address**: Enter the host address for the Technical Support Center.
 - **Support Token**: Enter the support token provided to you by the support staff.
2. Select **Connect**. The connection Status displays Connected.

If you are unable to open a TSC connection, your server may be located behind a firewall that prevents remote access to your site. Contact your network administrator to open the appropriate ports.

Support engineers may also guide you through alternative methods, such as HTTP tunneling, for remotely accessing your device.

Diagnostic Tools

From **Help & Troubleshooting > Diagnostic Tools**, capture and collect relevant system data used by technical support to troubleshoot issues.

Performing data capture testing sessions

From **Help & Troubleshooting > Diagnostic Tools**, capture system logs and network packets during a test session. The results of data capture can be used by technical support staff to diagnose issues.

To perform a data capture testing session, perform the following steps.

1. Go to **Help & Troubleshooting > Diagnostic Tools**, and select **Start**. The Start Data Capture dialog displays.
2. Complete the following fields:
 - **Maximum Capture Time**: Enter in minutes how long the data capture will last. The default value is 5 minutes.
 - **Enable**: In **Log Capture**, select **Enable** to turn on log capture.
 - **Log Level**: Select the log level to be set for the log capture.
 - **Enable**: In **Packet Capture**, select **Enable** to turn on packet capture.
 - **Interface**: Select the interface to be filtered for the packet capture.
 - **Host Address**: Enter the host address to be filtered for the packet capture.
 - **Port**: Enter the port number to be filtered for the packet capture.
 - **Enable**: In **System Report**, select **Enable** to include the system report in the capture.

3. Select **OK**. The data capture starts.
4. Perform the appropriate actions for the test session, such as send a study, receive a study.
5. Select **Stop** when the test is complete.
6. Download the result file by selecting **Download** next to the result file.
7. Delete the result files by selecting **Delete** next to the result file. Select **Delete All** to delete all the result files.

Generating diagnostic reports

From **Help & Troubleshooting > Diagnostic Tools**, generate diagnostic reports that contain information pertaining to your server hardware, storage configuration, and some system logs that may be useful for diagnosing potential issues with the server.

The system can maintain up to five of the most recent generated diagnostic reports.

To generate a diagnostic report, perform the following steps.

1. Go to **Help & Troubleshooting > Diagnostic Tools > Diagnostic Reports** tab.
2. Select **Create Report**. The report generates, but it may take a few minutes.
3. Save a copy of the report to your workstation by selecting **Download** next to the report.
4. Delete a report by selecting **Delete** next to the report you want to delete.

Network Tools

From **Help & Troubleshooting > Network Tools**, perform simple network tests and view a list of concurrent network connections.

Performing network connectivity tests

From **Help & Troubleshooting > Network Tools**, assess the network connectivity of your PACS appliance using the following tests:

- **Ping**: This test checks your connectivity from the PACS appliance to another server or appliance on the network.
- **Trace Route**: This test shows the path of networks used to access another server or appliance from the PACS appliance.

Both tests can provide response times in milliseconds, which can be useful in demonstrating the network speed between the PACS appliance and a selected network destination.

To perform network connectivity tests, perform the following steps.

1. Go to **Help & Troubleshooting > Network Tools**.
2. From the **Specify host address** dropdown list, select the host, or enter the valid host address of the destination you would like to test.
3. Select **Ping** or **Trace Route**. The test runs, and the test results display in the text box on the page.
4. Select **Stop** to stop a test that is in progress.

Network Activity

From **Help & Troubleshooting > Network Activity**, view all concurrent network connections.

Select **Refresh** to display the current network activity.

Server Logs

From **Help & Troubleshooting > Server Logs**, check server logs that the PACS appliance maintains for all of its services. Server logs may be useful for troubleshooting possible errors. Before contacting technical support, check the logs for possible errors.

Viewing logs

In addition to the current log, the system will maintain up to ten backlogs for each service.

To view (and download) logs, perform the following steps.

1. Go to **Help & Troubleshooting > Server Logs > View Logs** tab.
2. From the **Service** dropdown list, select the service whose logs you want to view. If you select All Services, the log combines only the most critical messages from all services. Additional messages may be provided by the logs for an individual service, depending on the logging level currently configured.

3. From the **Log** dropdown list, select the log you would like to view. Options depend on the service you select.
4. Select **View**. The log contents load in your browser.
5. Export the log file to your workstation by selecting **Download**.

Viewing per-association logs

From **Help & Troubleshooting > Server Logs > Per-Association Logs** tab, view per-association logs for the DICOM Service, MWL Tracker, and Routing/Fetching Service.

To view (and download) the per-association logs, perform the following steps.

1. Go to **Help & Troubleshooting > Server Logs > Per-Association Logs** tab.
2. From the **Service** dropdown list, select the service whose per-association logs you want to view.
3. Complete the following fields:
 - **DICOM Operation**
 - **From AE Title**
 - **To AE Title**
 - **Date/Time**
4. Select **View**. The per-association log contents load into your browser.
5. Export the per-association log file to your workstation by selecting **Download**.

Configuring logging levels

From **Help & Troubleshooting > Server Logs > Log Levels** tab, configure the logging level for specific services. This may be useful for troubleshooting or for providing additional information to technical support.

For each service, choose to turn on the most critical messages (INFO) or to turn on more detailed logs (DEBUG).

To configure the logging levels, perform the following steps.

1. Go to **Help & Troubleshooting > Server Logs > Log Levels** tab.
2. Select the logging level for each service.
3. Select **Save** to commit your changes.
4. Restore the logging levels for all services to their defaults by selecting **Reset**.

Setting up remote syslog logging

From **Help & Troubleshooting > Server Logs > Remote Syslog** tab, configure the PACS appliance to send its log messages to a remote syslog server. This may be useful for consolidating the log messages from multiple PACS appliances for analysis. You are responsible for setting up the remote server; consult your IT administrator.

To set up remote logging, perform the following steps.

1. Go to **Help & Troubleshooting > Server Logs > Remote Syslog** tab.
2. Select **Enable**.
3. Complete the following fields:
 - **Remote Syslog Host**: Enter the host address of the remote syslog server you have already set up for your site.
 - **Remote Syslog Facility**: Select the syslog facility to use for all log messages from this PACS. Your remote syslog server will filter the log messages it receives based on this setting.
4. Select **Save**.

Documents

From **Help & Troubleshooting > Documents**, view reference documents for the PACS system.

Study transfer measurements

The following study transfer measurements are theoretical calculations, not actual measurements. Use the information as a guide to plan resources to ensure you have sufficient bandwidth to maintain system operations.

Theoretical study transfer rate based upon bandwidth

Bandwidth	Transfer rate
1000 Mb/s	29.50 MB/sec
100 Mb/s	12.59 MB/sec
20 Mb/s	2.39 MB/sec
10 Mb/s	1.20 MB/sec
4 Mb/s	474.14 KB/sec
2 Mb/s	236.02 KB/sec
512 Kb/s	58.30 KB/sec

Theoretical time to transfer data based on Ethernet speed

Speed	10 Mbps	100 Mbps	1000 Mbps
1MB	< 1s	< 1s	< 1s
2MB	1.66s	< 1s	< 1s
5MB	4.17s	< 1s	< 1s
10MB	8.33s	< 1s	< 1s
20MB	16.67s	1.59s	< 1s
50MB	41.67s	3.97s	1.69s
100MB	1m 23s	7.94s	3.39s
200MB	2m 47s	15.89s	6.78s
500MB	6m 57s	39.71s	16.95s
1GB	14m 13s	1m 21s	34.71s

Theoretical time to transfer data based on connection bandwidth

Speed	512 Kbps	2 Mbps	4 Mbps	20 Mbps
100KB	1.72s	<1s	<1s	<1s
200KB	3.43s	<1s	<1s	<1s
500KB	8.58s	2.12s	1.05s	<1s
1MB	17.56s	4.34s	2.16s	<1s
2MB	35.13s	8.68s	4.32s	<1s
5MB	1m 28s	21.69s	10.80s	2.09s
10MB	2m 56s	43.39s	21.60s	4.18s
20MB	5m 51s	1m 27s	43.19s	8.37s
50MB	14m 38s	3m 37s	1m 48s	20.92s
100MB	29m 16s	7m 14s	3m 36s	41.84s
200MB	58m 33s	14m 27s	7m 12s	1m 24s
500MB	2h 26m 22s	36m 09s	18m	3m 29s

Speed	512 Kbps	2 Mbps	4 Mbps	20 Mbps
1GB	4h 59m 46s	1h 14m 03s	36m 52s	7m 08s

License agreement and warranty

The following license agreement appears when the web administration interface is accessed for the very first time. The user must accept the license agreement before using the software.

This license agreement must be accepted by an authorized representative of the user of this product prior to continuing this installation process. If you are a VAR or a SE (System Engineer), please insure that the user has accepted this license agreement prior to continuing.

License agreement and warranty for PACS appliances utilizing software and/or hardware

Important Read carefully before opening this package or using the software in any way: Opening this package or using this software in any way indicates your acceptance of these terms and conditions and is a representation by you that you have the authority to accept them. If you do not agree with these terms and conditions, you should promptly return the unopened package and your money will be refunded.

This End-User License Agreement and Warranty ("Agreement") is a binding legal agreement between you (either an individual or a legal entity) and Candelis, Inc. ("Candelis"). By opening this Candelis software (the "Software") package or by using the PACS appliance and associated hardware products (the "Hardware") and the Software in any way, you agree to be bound by the terms of this Agreement. (The term Software includes the computer software, the associated media, any printed materials, and any "online" or electronic documentation and any updates we provide to you in the future.) If you do not agree to the terms of this Agreement, Candelis is unwilling to license the Software to you. In such event, you may not install, use or copy the Software, and you should promptly contact your retailer for instructions on return of the unused product(s) for a refund.

Software license and warranty

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed to you, not sold. Candelis retains all right and title to the Software and related documentation.

Grant of license: This Agreement grants you the following rights: - **Software:** You may install and use one copy of the Software on one server computer. In addition, any license, if applicable, is valid for no more than the number of concurrent users for which the license is purchased. For iMed-Stor products, the license, if applicable is valid for no more than the number of remote AE titles for which the license is purchased. - **Backup copy:** You may not make back-up copies of the Software. During the period of this license, or any paid support period, if you require a copy, Candelis will provide a copy to you.

Description of other rights and limitations: Limitations on Copying and Distribution: Except as provided in section 1 above, you may not copy, transmit, or distribute the Software, except and only to the extent that such activity is expressly permitted by applicable law despite this limitation. You may not modify the Software to increase the number of allowed concurrent users or if applicable, remote AE titles.

Limitations on reverse engineering and modification: You may not reverse compile, reverse engineer, decompile, disassemble, convert to a humanly comprehensible form, modify or create works derivative of the Software. You may not disguise, obfuscate or attempt to use the Software in order to use it elsewhere. You may not tamper with the operating system or any keylock or copy protection features or use the Software in a manner or for a task it was not designed to operate. If the Software is serialized, you may not modify or disable the serial number features nor copy protection mechanisms contained in the Software.

Separation of components: This Software is licensed as a single product for use with the hardware that accompanies the Software. You may not add additional hardware components to those which accompany the Software at the time of sale. The addition of additional storage, memory or other hardware to the Software and the Candelis hardware will be a violation of this license agreement and the remedies shown in "Termination" shall apply. The components of the Candelis Hardware and Software may not be separated for use on more than one computer.

Sublicense, rental and third-party use: You may not sublicense, rent, and timeshare, loan or lease the Software, or directly or indirectly permit a third party to use or copy the Software.

Software transfer: You may permanently transfer your rights under this Agreement, provided you (i) retain no copies; (ii) transfer all of the Software (including all components, the media, all printed materials, any upgrades, and this Agreement); (iii) provide Candelis with written notice of the transfer within ten (10) days; and (iv) obtain and provide Candelis with the written consent of the third party to abide by the terms and conditions of this Agreement. Any other assignment by you of this agreement shall be void. If the Software is an upgrade, any transfer must include all prior versions of the Software.

Termination: Without prejudice to any other rights, Candelis may terminate this Agreement if you fail to comply with the terms and conditions set forth in this Agreement. In such event, you must return all copies of the Software and all of its components and documentation to Candelis or certify that you have destroyed all such copies. In such event, the license to use the Software will be terminated and Candelis may enjoin any user of the Software from further use. Candelis will vigorously enforce its license, copyrights and other legal rights. In addition to terminating the license, Candelis may refuse to provide any continuing warranty service or repair. A termination of the license also serves to void the warranties on the Software and the Candelis Hardware.

Export: You may not export the Software without prior written approval from Candelis. If the Software was purchased in the United States of America, you agree to comply with all applicable United States laws and regulations pertaining to export controls. If the Software was purchased outside the US, you may not re-export the Software except as permitted by the laws of the United States and the laws of the jurisdiction in which you purchased the software.

Copyright and ownership: All title and copyrights in and to the Software, including, but not limited to, any images, photographs, animations, video, audio, music, text, incorporated in the Software, the accompanying printed materials, and any copies of the Software, are owned by Candelis or its suppliers. You may not copy the printed materials accompanying the Software.

Statement of use: You acknowledge that you are not utilizing the Software to diagnose or treat medical conditions, and that all of your use of the Software will be fully compliant with any laws and regulations. Specifically, You acknowledge that HIPAA compliance is your responsibility and further, You acknowledge that you will not use the Software in any manner in which You do not fully comply with any HIPAA statutes and/or regulations. You acknowledge that HIPAA requires that you maintain backup copies of all patient data in duplicate locations.

Limited warranty: Candelis warrants that the Software will perform substantially in accordance with the applicable Candelis published documentation prevailing at the time of shipment for a period of ninety (90) days from the date of receipt, and that the Hardware will perform substantially in accordance with the applicable Candelis published documentation prevailing at the

time of shipment for a period of one (1) year from the date of receipt, unless a different warranty period has been offered in writing. Candelis warrants that any media accompanying the Software will be free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of receipt. Any implied warranties on the Software and media are limited to ninety (90) days. Some states or jurisdictions do not allow limitations on the duration of an implied warranty, so the above limitation may not apply to you.

Customer remedies: Candelis entire liability and your exclusive remedy shall be, at Candelis option, either (a) return of the price paid, or (b) repair or replacement of the Software or Hardware that does not meet the limited warranty in Section 6 above and which is returned to Candelis with a copy of your receipt. Any replacement Software or Hardware will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

No other warranties: You acknowledge and agree that the use of the software and/or the hardware is at your own risk. To the maximum extent permitted by applicable law, Candelis and its suppliers disclaim all other warranties, either express or implied, including, but not limited to, implied warranties of non-infringement, merchantability and fitness for a particular purpose. Candelis does not warrant that the functions contained in the software or hardware will meet your specific requirements, or that the operation of the software will be uninterrupted or error-free, or that defects in the software and related documentation will be corrected. Furthermore, Candelis does not warrant or make any representations regarding the use of the results of the use of the software or related documentation in terms of their correctness, accuracy, reliability, or otherwise.

No oral or written information or advice given by Candelis or a Candelis authorized representative shall create a warranty or in any way increase the scope of this warranty. This limited warranty gives you specific legal rights. You may have others which vary from state or jurisdiction to state or jurisdiction.

No liability for consequential damages: To the maximum extent permitted by law, in no event shall Candelis or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of data, loss of images, loss of business profits, business interruption, loss of business information, loss of medical information, corruption of medical information, misdiagnosis of a medical condition, loss of image quality, loss of image fidelity, violation of HIPAA laws and regulations or any other loss) arising out of the use or inability to use the software or the hardware, even if Candelis has been advised of the possibility of such damages. In any case, Candelis's entire liability under any provision of this agreement shall be limited to the price paid for the software or the hardware prorated for your period of use, up to a maximum of 24 months. Because some states or jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Data storage, backups, and updates: Candelis requires that you maintain an effective system to ensure that your data and images are backed up routinely and frequently to prevent data loss, that backup media is stored in a location geographically separate from that of the system that is being backed up, that backup procedures commence immediately upon system installation and that both backup and restore operations are tested regularly to provide for the highest probability of accurate and complete data recovery. You acknowledge that Candelis may refuse to provide system updates, software patches, archive expansion, data migration, installation or routine service to the Software unless you have maintained, and are maintaining, an effective backup system. You agree that if Candelis offers updates to the Software, you will allow such updates, including access to your system and network where necessary, and if you do not arrange such access for such updates, the warranties will no longer apply to the Software. You agree that Candelis shall not be responsible for any inherent conflicts between your operating systems and the Software and its updates, if any, or for any damage, data loss or condition which arises during or occurs as a consequence of such update.

Data integrity and compression: You acknowledge that the PACS system may utilize various methods and techniques to compress images. You acknowledge that if certain compression techniques are utilized, you will experience a loss of image quality. Candelis is not responsible for the degradation of any image quality or when lossy compression or other compression techniques are utilized. Where specific PACS features modify any images (such as CLAHE, MIP, MPR and the like), you must rely on the original image as acquired by the modality.

Indemnity: The Software is not intended to replace the skill and judgment of a qualified medical practitioner and should only be used by people that have been appropriately trained in the Software's functions, capabilities and limitations. For example, and without limitation, various functions of the Software, including CLAHE, Maximum/Minimum Intensity Projection (MIP), Multi-Planar Reconstruction (MPR) and the like, are intended for use only as an adjunct to two-dimensional medical image display techniques. You agree to hold harmless, indemnify and defend Candelis, its suppliers, officers, directors and employees, from and against any personal injury or property damage or other losses, damages, fines and expenses (including attorneys' fees and litigation costs) arising out of or relating to your use of the Software. **The entire risk arising out of your use of the software and documentation remains with you.**