

English

System Admin Guide

300018593821_A

Philips Advanced Image Insights solution

Version 1.0.1 2026-09-10

Table of Contents

1 Before You Begin 5
Performance Characteristics 5
Compatibility 5
Compliance 6
Safety 6
Network Safety, Security, and Privacy 7
Regulatory Controls 8
Software Updates 8
Security Issues and Guidelines 9
Implemented Security And Privacy Features 10
Additional Security and Privacy Features 10
Malware Protection 12
Microsoft Security Updates 12
De-identification 13
Data Sanitization 13
Unsecured Personal Data Transmission Risks 14
Safe Disposal of Software Components 14
Ordering Printed Instructions for Use 14
2 Login Setup 15
3 PACS Integration 19
4 Relevancy Definition 33
5 Audit 35
6 AIO Configuration 37
7 Monitoring the workflow (data and application) via dashboard 45

300018593821_A/881 * 2026-09-10

Table of contents

300018593821_A/881 * 2026-09-10

Philips

1 Before You Begin

Performance Characteristics

Philips Advanced Image Insights on HealthSuite (AII) is a cloud-based solution that integrates a broad portfolio of clinical applications into radiology and cardiology point-of-care devices and workflows such as PACS and imaging systems (MR, CT, IGT). It provides a single access point to a broad portfolio of both Philips and third-party AV/AI solutions. The application portfolio spans across all clinical domains, including cardiology, oncology, neurology, pediatrics, women's health, and administration and work with data from all imaging modalities.

Advanced Image Insights works with multivendor, multi-modality data and support the data sources and data types required by the AV/AI applications and point-of-care devices (PACS, MR, CT, IGT, DXR, US, etc.).

Advanced Image Insights solution supports:

- Philips PACS, on-prem and on-cloud, with AV-on-cloud and headless third-party AI applications, including Accept/Reject workflow
- Workstation mode with AV-on-cloud applications
- Third-party PACS with AV-on-cloud and third-party AI applications, with limited integration supported via standard DICOM and HL7 interface

For application specific performance characteristics, please refer to the Measurement Accuracy section of each application that includes measuring function. For applications that do not include a measuring function for performance characteristics, please refer to the Indications for Use section of each application.

Note: The screenshots in the Instructions for Use can differ from the user interface screens on details. The screens captured in these Instructions for Use may not reflect the latest User Interface coloring of the product, however the Instructions For Use remain applicable in all other aspects.

Compatibility

The software product ("Philips Advanced Image Insights solution") described in this Instructions for Use communicates with other products using the DICOM-3 standard (e.g. with imaging systems of different modalities). Philips Advanced Image Insights solution uses the DICOM protocol to receive and send lossless images as described in the DICOM Conformance statement.

Receiving the ORM messages from HIS/RIS is not supported. Only HL7 results generated by the AI applications are sent to the configured PACS system via DICOM Gateway.

300018593821_A/881 * 2026-09-10

Philips

Your local Philips representative or manufacturer can be contacted for any questions regarding compatibility with specific devices and/or components. Information on significant restrictions related to compatibility can be found in the Release Notes accompanying this Instructions for Use. Philips is not responsible for running compatibility validation of non-supported third-party software.

Any addition or change to software products installed on the on-prem components or changes of operating system configuration is restricted unless the other software equipment or components are recognized as compatible by Philips. A list of such software, equipment and components is available on request from your local Philips Representative, or the Manufacturer. Philips is not responsible for running compatibility validation of non-supported third-party software.

Any changes and/or additions must comply with all applicable laws and regulations that have the force of law within the jurisdiction(s) concerned, and with best engineering practice.

Changes and/or additions carried out by persons without the appropriate training, and/or using unapproved spare parts, may lead to the Philips Health Systems warranty being voided. Philips is not responsible for any malfunction of Philips Advanced Image Insights solution, if Philips Advanced Image Insights solution runs on hardware that is not according to hardware specifications. If not supplied by Philips with the Philips Advanced Image Insights solution software, Philips is not responsible for any malfunction of the hardware used. As with all complex technical equipment, Solution maintenance by persons not appropriately qualified and/or using unapproved spare parts carries serious risks of damage to the equipment and of personal injury.

300018593821_A/881 * 2026-09-10

Compliance

The Philips Advanced Image Insights solution complies with relevant international and national standards and laws. Information on compliance is supplied on request by your local Philips representative, or by Manufacturer. This software solution shall be installed on appropriate IT equipment that complies with relevant international and national laws and standards on EMC (Electro-Magnetic Compatibility) and Electrical Safety. Such laws and standards define both the permissible electromagnetic emission levels from equipment and its required immunity to electromagnetic interference from external sources.

Safety

Philips products are designed to meet stringent safety standards. However, all software medical devices require proper operation and maintenance, particularly with regard to human safety.

It is vital that you follow strictly all safety directions under the heading **Safety** and all **Warnings** and **Cautions** throughout this "Instructions for Use", to help ensure the safety of both patients and operators.

In particular, you must read, understand and know the information described in this Safety section before using this device.

You should also note the following information:

Philips

- Intended use of Philips' Advanced Image Insights (AII). See the AII System Instructions for Use section "Intended Use".

NOTICE

Any serious incident that has occurred in relation to the device should be reported to the manufacturer and the competent authority of the Member State in which the user and/or patient is established.

Network Safety, Security, and Privacy

Philips recognizes that the security of Philips products is an important part of your facility's security-in-depth strategy. However, protection can only be realized if you implement a comprehensive, multi-layered strategy (including policies, processes, and technologies) to protect information and systems from internal and external threats.

Following industry-standard practice, your strategy should address:

- Physical security, e.g., do not allow unauthorized people to use Advanced Image Insights (AII), and maintain appropriate network security measures to protect AII and its associated infrastructure.
- Operational security, e.g., make sure that any sensitive information left on the system—such as exported files—is removed, and make sure that users of AII do not leave the open system unattended.
- Procedural security, e.g., create awareness of the dangers of social engineering, give every single user a separate account, and do not forget to remove an account when it is no longer needed.
- Risk management
- Security policies, e.g., make sure that the AII Service Documentation and media are securely stored.
- Contingency planning

The practical implementation of technical security elements varies by site and may employ a number of technologies, including firewalls, virus-scanning software, authentication technologies, etc.

As with any computer-based system, protection must be provided so that firewalls and/or other security devices are in place between the medical system and any externally accessible systems. The USA Veterans Administration has developed a widely used Medical Device Isolation Architecture for this purpose. Such perimeter and network defenses are essential elements in a comprehensive medical device security strategy.

Any device connection to an internal or external network should be done with appropriate risk management for product effectiveness and data and systems security. Additional security and privacy information can be found on the Philips product security website at:

www.philips.com/productsecurity

300018593821_A/881 * 2026-09-10

Please review Philips product security policies regarding remote service, patch management, anti-virus software and more in the “Product Security Policy Statement” and additional information sources available through this website.

NOTICE

Philips is not responsible for the security of hospital-managed systems (desktop PCs, laptops) where the Philips Advanced Image Insights solution gateway server is installed.

Regulatory Controls

Protect Patient’s Health Information

One of the most important assets to protect with security measures is the patient's health related information.

Many governments require Solution maintaining the confidentiality of this information. Therefore, strict security measures must be taken to guard this protected information.

NOTICE

Users in the U.S.A. may find guidelines at http://www.hhs.gov/ocr/hipaa/.

Prevent Unauthorized Device Modification

Philips sells highly complex medical devices and systems. We are required to follow government-regulated quality assurance procedures to verify and validate modifications to the operation of our solution.

Software Installation

CAUTION

Installing software not authorized by Philips, or not specified in the system documentation for Philips' Advanced Image Insights solution, may adversely affect the operation and security of the system, as well as the networks to which the system is connected. These adverse effects may not be immediately apparent to the user. Therefore, users should not install unauthorized software onto the Philips Advanced Image Insights solution gateway server.

Software Updates

Updates for this Philips software product can become available. Such updates are essential to keep the software product operating safely, effectively, and reliably.

300018593821_A/881 * 2026-09-10

Philips

Security Issues and Guidelines

In addition to the patient information and device integrity, needs discussed in the preceding section on regulatory requirements, the following topics, issues, and guidelines should be understood and addressed by operators and owners. This applies Philips Advanced Image Insights solution and not the client PCs.

Network Security

The Philips Advanced Image Insights solution (gateway server) must be placed on a secure local computer network that has protections against viruses and other harmful computer system intruders. Make sure the equipment is connected to a local network that uses appropriate protection, such as a firewall and virus scanners.

If you suspect a cybersecurity incident, including unauthorized access, malware infection, unusual device behavior, or other security concerns, contact local Philips representatives or visit Philips' security information page.

Remote Service

Remote Service provides a set of tools that enable Philips to perform monitoring and service actions, entirely or partly, from a remote location. Remote Service is designed to reduce system downtime and improve investigation of systemic issues.

Remote Service features include:

- automatically generated alerts for usage of Advanced Image Insights server hard disk space
- remote assistance for workstations
- distribution of critical product software patches
- software distribution
- connectivity alerts
- miscellaneous alerts

Room Access Control

Procedures must be put in place to limit physical access to the product/solution, to prevent accidental, casual or deliberate contact by unauthorized individuals.

Access to the room containing the Philips Advanced Image Insights solution gateway server should be controlled by policy and procedures that identify who is authorized to occupy specific areas. Check with your hospital’s Safety and Security Office for more information on what measures are in place or how to implement room access controls.

User Login and Logout Protections

A consistent user login process (user names and passwords) provides good security of protected information. Minimum login standards include:

300018593821_A/881 * 2026-09-10

- Implementing strong passwords. This is the easiest and most effective method to increase security. Strong passwords consist of at least eight alphanumeric, mixed case characters, digits, and special characters like "@" or "*".
- Never use words that can be found in the dictionary.
- Never post or share user names and passwords.
- Change passwords periodically.

Implemented Security And Privacy Features

It is the policy of Philips to adhere to all required standards and regulations. To assist the hospital in fulfilling security and privacy requirements such as the Health Insurance Portability and Accountability Act (HIPAA) requirements, introduced by the United States Department of Health and Human Services, functionality has been added to the Philips Advanced Image Insights solution.

Access Control

Intended to restrict access to the system to authorized users only:

- A user log-on/log-off procedure is required to gain access to the system.
- Access to the system is granted according to a customizable list of authorized users.
- Only username/password authentication is supported.
- Password complexity rules are defined as per Philips standard.
- Password expiration rules is defined as per Philips standard
- Account Lockout Policy is defined as per Philips standard.
- Customers need to notify Philips for onboarding, offboarding, permissions, etc.

Audit Trail

Required to log user activities which are information-security critical:

- Applies to logging-on, reading and/or modifying clinical information.
- The audit trail logs can be viewed by customer via audit log web application. Contact a Philips representative to request access.

Additional Security and Privacy Features

HIPAA defines a number of physical and technical safeguards which are either required or addressable. Some features that could implement these functions are different or not implemented for reasons mentioned below. This section also lists other information related to security features that are not implemented and that the owner of the systems should be aware of.

300018593821_A/881 * 2026-09-10

Philips

Backup Procedure

The system is not intended for permanently storing sensitive patient personal information. Information should be exported to a long-term storage device as soon as possible.

Emergency Access Procedure

The Philips Advanced Image Insights solution system does not have a built-in emergency user account. However, it supports the creation of unique user accounts and assignment of permissions to users.

It is not possible to clearly mark data output (e.g., screen, print-out and exported data to DVD) as having been created during an emergency access operation.

Encryption

Windows BitLocker, a full disk encryption feature (provided by the Windows OS) that protects data by encrypting entire volumes, can be enabled by the Hospital Administrator as needed, to encrypt data at rest on the Philips Advanced Image Insights gateway server.

For data in transit, the Philips Advanced Image Insights solution system supports the IH EATNA profile, which enables secure transmission of ePHI between configured DICOM devices.

NOTICE

It is the responsibility of the users to keep their password secret.

Physical Access to System

The Philips Advanced Image Insights solution (gateway server) should be placed in an access-restricted area in the hospital. However, the following characteristics are to be taken into account for system operation and access control:

- The computer case is "service friendly", e.g., accessing and removing the hard drive does not require tools. However, the computer case can be locked, e.g., by cable lock.
- The boot order for the system is DVD, USB, hard disk. By inserting bootable a CD/DVD or connecting a bootable USB memory device, the system may start up from those and thus access may be gained to the system, including information stored in it.
- There is no detection of unauthorized physical access into the system. e.g., through tamper-proof seals.
- Unauthorized changes to software, files or data on the Philips Advanced Image Insights solution system are not permitted, and doing so may adversely affect the operation and security of the system.
- The system BIOS is not password protected and can be accessed during startup of the system if unauthorized access to the system is possible.

300018593821_A/881 * 2026-09-10

Philips

NOTICE

Make sure that in the BIOS of the Philips Advanced Image Insights Server, the option to boot from CD is not enabled.

Malware Protection

The Philips Advanced Image Insights solution (gateway server) incorporates protection mechanisms against the intrusion of malware (viruses and so on). Without proper cyber security, the effectiveness of these provisions may degrade over time since malware is continuously altered to target newly discovered vulnerabilities.

Despite preventive measures already implemented, a remote possibility exists that the equipment may become infected with malware. When malware is detected, or when you notice that unfamiliar behavior or degraded performance occurs repeatedly, including after switching the system off and on again, you should call the Philips Service Engineer for an inspection.

If the inspection confirms infection, be sure to take measures to contain and remove the source of infection. Service will reinstall the product`s software to bring the product back into specification.

NOTICE

Although the system incorporates state-of-the-art protection mechanisms to protect it against the intrusion of malware (for example, viruses), there is a remote possibility that a system can become infected. System safety is guaranteed in all circumstances, but the user might notice unfamiliar system behavior and/or performance. If this happens repeatedly, e.g. also after the system has been switched off and on again, the user is advised to contact a Philips Healthcare service representative to have the system checked and, if needed, to remove the malware. External circumstances can influence the availability of the clinical data, e.g. network failure, power failures, environmental disasters, etc.

Philips-Certified Anti-virus Software

Philips recommends that you should implement one of the following certified, industry-recognized anti-virus solutions, as an additional level of protection, coupled with the standard allow listing already provided. The implementation of a certified anti-virus software solution on Philips Advanced Image Insights solution (gateway server) enables customers to maintain system protection in line with the local IT policy.

Updating and operational management of the anti-virus solution and its virus definition file(s) is the responsibility of the customer. Philips supports any standard anti-virus software.

Microsoft Security Updates

Microsoft Security Updates are routinely included with each new software release. Alternatively, Philips permits Philips Advanced Image Insights solution customers to install Microsoft security updates on the Gateway server and the Client PC/Workstations.

300018593821_A/881 * 2026-09-10

Philips

For a list of approved/validated Microsoft® security updates for the Philips Advanced Image Insights solution, refer to the vulnerability evaluation report, which are referred to as Security Status document(s). The document(s) are accessible via the following link:

www.philips.com/security

Once the web page loads, select the option/image for “Cyber-security information of Philips healthcare products”. A new web page opens. Follow the guidelines provided to first request access to the product security documentation, and subsequently to access the document distribution platform, Philips InCenter.

On Philips InCenter, look for the product group “Imaging Clinical Applications and Platform (ICAP)” to find the Security Status document(s) for the Philips Advanced Image Insights solution product with reference to the Security Status document, Philips permits customers to install only security updates which have the “Recommended Customer Action” as “Install recommended solution”.

For each of these approved security updates, the Security Status document mentions the Knowledge Base (KB) Article related to each security update.

De-identification

The De-identify option enables you to save images while removing any identifying marks of the patient, such as patient name and patient ID.

Details of de-identified tags can be found in the DICOM Gateway DICOM Conformance Statement.

Data Sanitization

Advanced Image Insights stores patient sensitive data within the system DICOM images. Media containing backups of the database and images will contain patient or sensitive data as well.

Patient, Personal or sensitive data can be stored in the following locations of the Advanced Image Insights in a temporary location:

- DICOM Store
- DICOM Gateway on cloud or on-premises
- AV on Cloud
- Third-party AI applications

For on-premises deployments, the Customer is responsible for performing data sanitization in accordance with their organizational policies and procedures. For cloud deployments, the Customer must notify Philips to initiate data sanitization. Philips will sanitize patient, personal, and other sensitive data from the cloud environment and can provide a Certificate of Destruction upon request.

300018593821_A/881 * 2026-09-10

Philips

NOTE

If patient data, images, or sensitive information resident on the system are to be discarded or permanently disposed of, they must be destroyed (permanently deleted) so that the data no longer can be accessed, retrieved, or viewed at a later point in time. Data sanitization must be performed for permanent deletion. While the solution has data deletion capabilities, it does not provide data sanitization functionality. Use appropriate data sanitization techniques and tools in alignment with healthcare entity policy and procedure for media destruction and sanitization. NIST publication 800-88 Guidelines for Media Sanitization provides reference and best practices for data sanitization.

Unsecured Personal Data Transmission Risks

Advanced Image Insights transmits and receives patient images and data over a network. Data that is transmitted in an unencrypted format over a network introduce unknown risks impacting confidentiality and integrity. To reduce the risk of unauthorized data exposure, Philips strongly recommends the use of TLS (TLS 1.2 / TLS 1.3) for all Web and DICOM services to ensure the secure transmission of data to the client device or modality. Note that the healthcare entity might need to purchase or provide valid TLS certificates.

Safe Disposal of Software Components

During hardware replacement or offboarding activities, it is the customer's responsibility to sanitize the software and securely remove any residual data from the systems.

Ordering Printed Instructions for Use

You can contact your local Philips representative for a printed IFU.

A printed IFU can be also obtained by:

- Personally printing the printable PDF file provided.
- Placing an order through the public website http://www.philips.com/IFU .

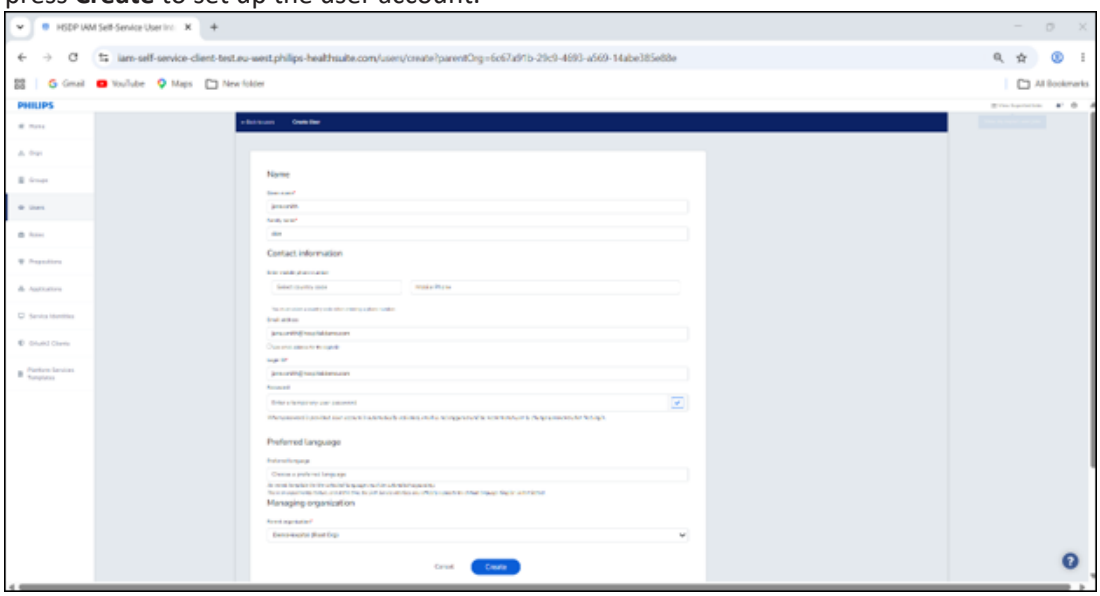
300018593821_A/881 * 2026-09-10

2 Login Setup

Create a user account in Identity Access Manager (IAM)

Prerequisites: To create a user account, you must have the following details: Given name, Family name, Email address, and Login ID.

1. Login to IAM Self Service Tool
   Note that the URL is specific to the region of deployment, and is provided by the Philips Service team.
2. From the **Organization** list, select the organization created for the customer under the IAM Root, and set the organization context.
3. Go to the **Users** tab, then select **+ Add User**.
4. Add the following details: Given name, Family name, Email address, and Login ID. Then press **Create** to set up the user account.



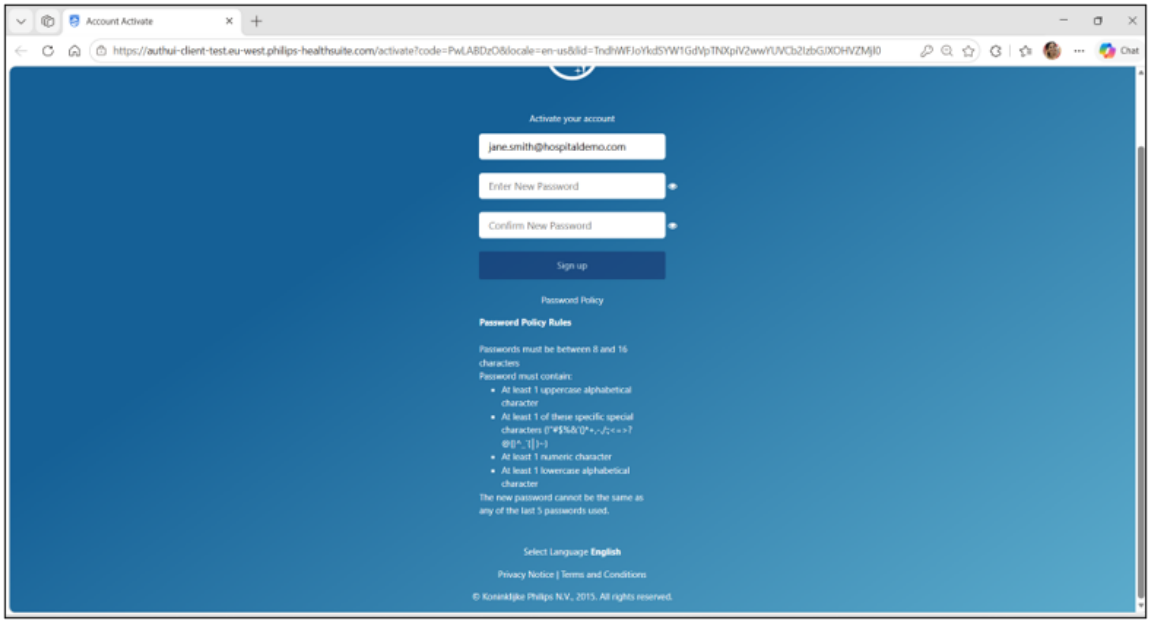
NOTE

Do not specify a default password. Before using the user account to log in, it must be activated. To activate a user account, see the following section.

Activate a user account

To activate the account, follow the steps listed in the AII System IFU in the section "User Account & Login", in the subsection "Activate a user account".

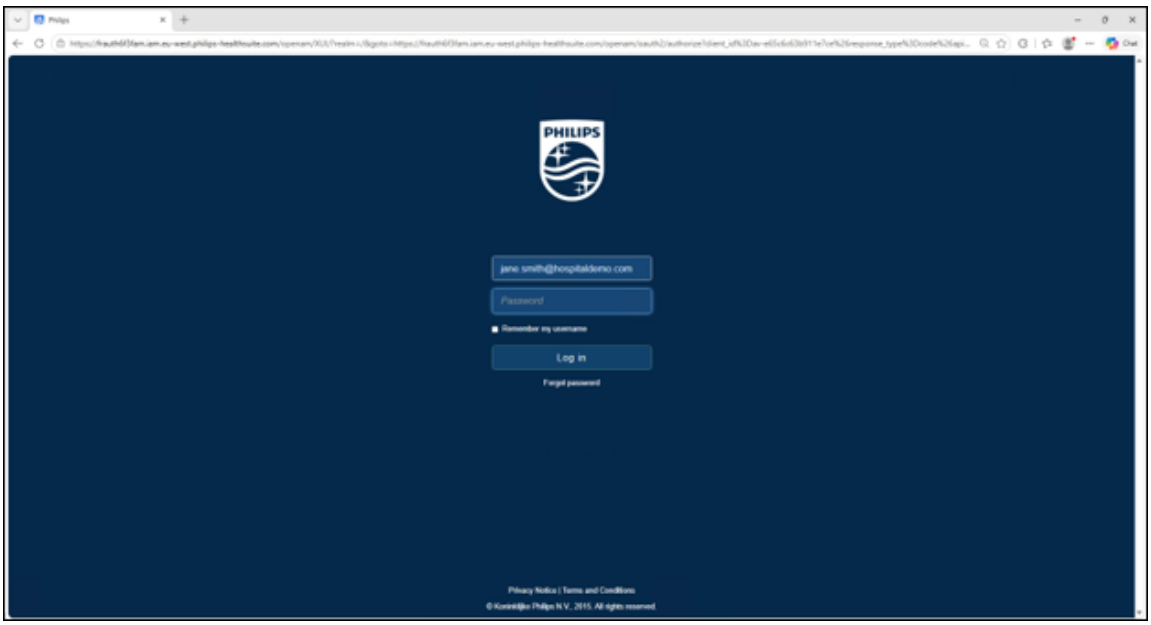
300018593821_A/881 * 2026-09-10



NOTE

If the user does not receive an activation email, the administrator can send an activation email by logging into the URL mentioned in Step 1 of the numbered list of the previous section "Create a user account in Identity Access Manager", and then selecting the customer organization and user account, and then from the upper-right options selecting **Resend activation email**.

Reset a password



To reset a password, follow the steps listed in the AII System IFU in the section "User Account & Login", in the subsection "Reset a password".

300018593821_A/881 * 2026-09-10

Alternatively, the administrator can trigger a password reset by logging into the URL mentioned in Step 1 of the numbered list of the previous section "Create a user account in Identity Access Manager", and then selecting the customer organization and user account, and then from the upper-right options selecting **Force a reset of the user’s password**.

300018593821_A/881 * 2026-09-10

300018593821_A/881 * 2026-09-10

Philips

3 PACS Integration

Setup PACS for DICOM communication

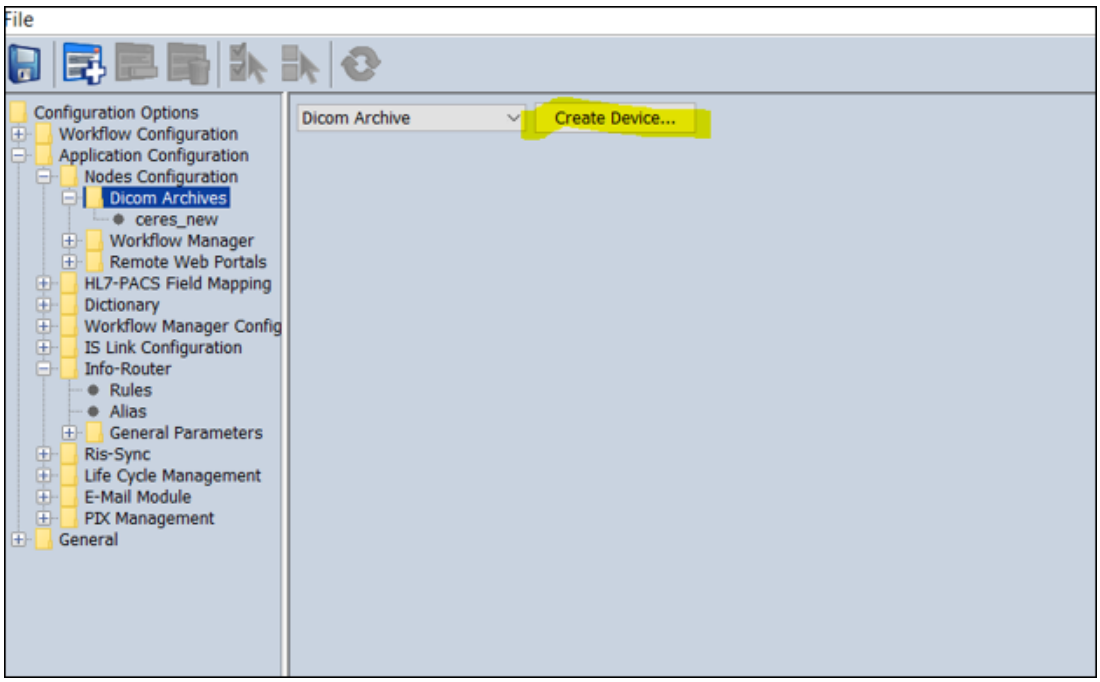
This section describes how to establish a DICOM network connection between the PACS and DICOM gateway, so that DICOM studies can be sent to the DICOM gateway and further for processing by the AV and AI applications.

Prerequisites

- IP address, AE title(s) , port (configured as 11112) of the DICOM gateway sending the data from PACS.

VUE PACS

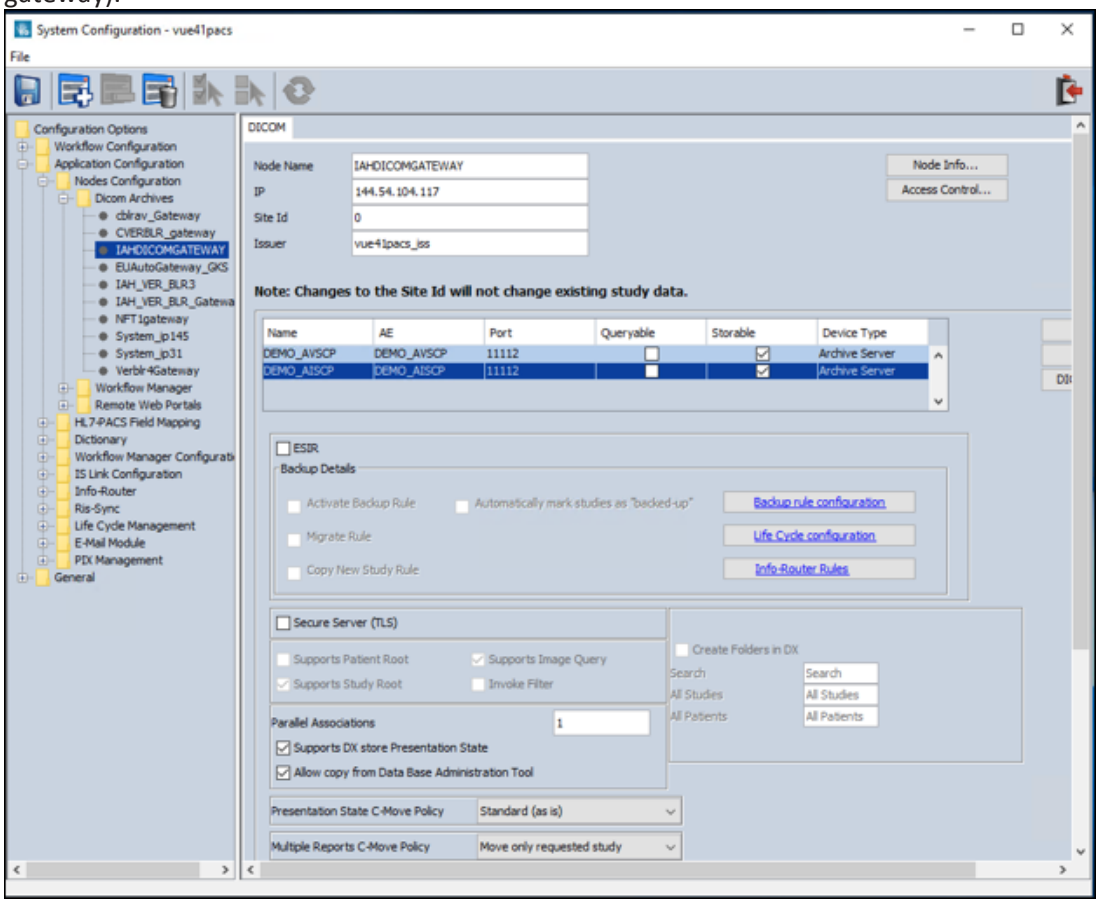
1. Log on to the Vue PACS server.
2. Go to: system configuration/Application Configuration/Nodes Configuration/Dicom Archives
3. Select **Create Device** and fill in the attributes and its values, as given in the table directly below this numbered list.



4. Add two entries for AE titles, as shown below:
   One AE Title is dedicated to sending data to AV applications (data sent to this AE Title will not be de identified at the DICOM gateway), while another AE Title is dedicated to sending

300018593821_A/881 * 2026-09-10

data to AI applications (data sent to this AE Title will be de identified at the DICOM gateway).



In the above case, DEMO_AVSCP:11112 and DEMO_AISCP:11112 represents the DICOM gateway node information that is used to forward studies.

DICOM node configurations can change from site to site. After making changes, save and restart the corresponding services.

Attribute	Default	Possible Values	Comment
Node Name	###	string	Indicates the name of Dicom Node. Add a new name like ‘aiidicomgateway’
IP	144.54.104.117	string	Indicates IP of DICOM gateway system
Site ID	Keep it Default	string	Site ID of this site
Issuer	Keep it Default	string	Issuer

ISPACS

1. Log on to ISPACS and launch Navigator in the browser.

300018593821_A/881 * 2026-09-10

2. Go to **DICOM** tab **> S/C SCP/**
3. Select **Add** and fill in the attributes for AE Title, IP Address, and Port.
4. Add 2 entries for AE titles, as listed below:
   One AE Title is dedicated to sending data to AV applications (data sent to this AE Title will not be de identified at the DICOM gateway), while another AE Title is dedicated to sending data to AI applications (data sent to this AE Title will be de identified at the DICOM gateway).

   In the above case, DEMO_AVSCP:11112 and DEMO_AISCP:11112 represents the DICOM gateway node information that is used to forward studies.
   DICOM node configurations can change from site to site. After making changes press **Save**.

Setup PACS for HL7 communication

To enable HL7 integration for AI applications on the PACS system, an HL7 template specific to the site and PACS must first be defined. Once the template is established, configuration is required both at the Advance Image Insights Solution (using the template) and at the PACS to ensure proper receipt and parsing according to PACS rules.

The HL7 receiving node details at the PACS must also be configured in the admin dashboard to allow the DICOM Gateway to transmit the information.

For further guidance on template setup and HL7 configuration, refer to the VUEPACS/ISPACS integration guide.

Configuration for the applications in Vue PACS

All external application configurations in Vue PACS are managed through the Central Configuration Editor.
Prerequisite: The following details should be available

- URL for the third-party AI applications' Accept Reject tool and AV
- Secret Key

Advanced Visualization (AV) applications

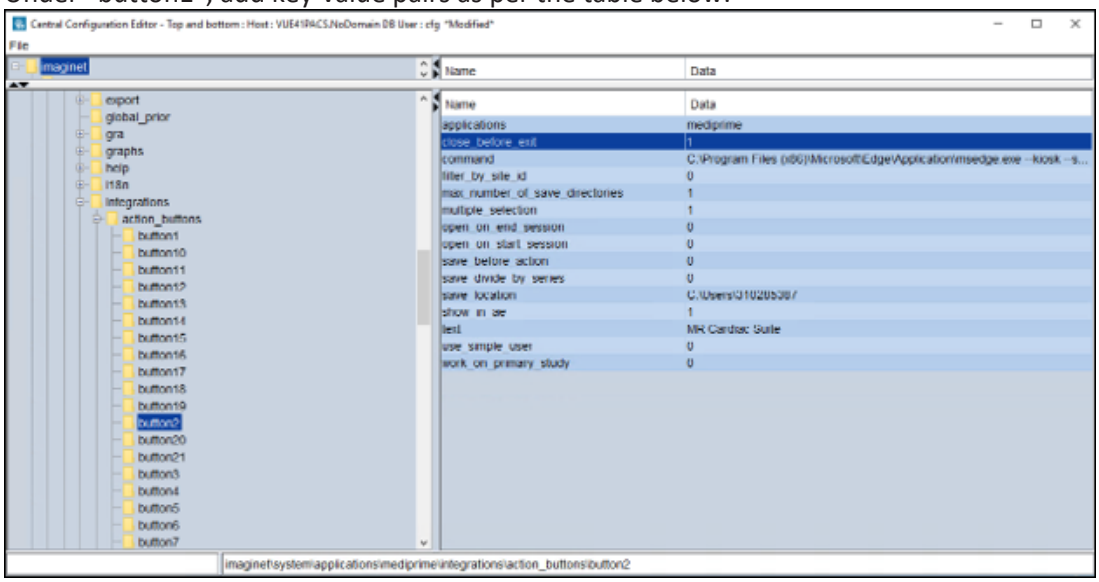
This section describes how to launch an AV application from PACS Diagnostic Viewer. There are two options: From the diagnostic viewer and From the patient jacket.

From the diagnostic viewer

1. Log on to the Vue PACS server.
2. Open the Central Configuration editor, Go to imaginet\system\applications\mediprime\integrations\action_buttons
3. There is a key for each action button. The format for each key is “buttonX”, where X is a number used to determine the Action Button position in the Action Buttons list in the application.

300018593821_A/881 * 2026-09-10

4. Under “button1”, add key-value pairs as per the table below:



Repeat these steps for all the applications that need to be configured.

Attribute	Value	Comments
applications	mediprime	The application where we would like to embed in.
command	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --kiosk --start-minmized "https://hscadapter_baseurl:5001/launch-ui.html?ApplicationName=app_name Suite&StudyUID=@STUDY_INSTANCE_UID@ &SeriesUID=@SERIES_INSTANCE_UID&ShowSeriesSelector="false"&applicationId=pacs_plugin"	Command for launching the AV application.
show_in_ae	1 or 0	Set value as 1 if the application needs to be listed under External Applications in the Worklist, and 0 otherwise.
text	MR Cardiac Suite	Name of the application to be displayed.
mulitple_selection	1 or 0	Set the value as 1 if multiple data selection needs to be enabled, and 0 otherwise.

300018593821_A/881 * 2026-09-10

Attribute	Value	Comments
Multi Studies Command	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --kiosk --start-minmized "https:// hscadapter _baseurl:5001/launch-ui.html?ApplicationName=app_name Suite&StudyUID=@STUDY_INSTANCE_UID@ &SeriesUID=@SERIES_INSTANCE_UID&ShowSeriesSelector="false"&applicationId=pacs_plugin	If the application supports multiple studies, configure the command to pass the selected study and series identifiers as part of the request URL.

Command Parameter Name	Comments
hscadapter_baseurl	URL of the service endpoint used for accessing the AV application. Use the hostname or fully qualified domain name (FQDN) of the gateway system if it is deployed on-premises. For cloud deployments, use the service URL provided by the operations team.
StudyUID	Mandatory, the value should always be set to @STUDY_INSTANCE_UID@. During application launch, this placeholder is automatically replaced with the UID of the selected studies.
SeriesUID	Optional, can be configured if the selected series needs to be passed from Vue during application launch. The value must always be set to @SERIES_INSTANCE_UID@ During application launch, this placeholder is automatically replaced with the UID of the selected series.
ApplicationName	Name of the AV application. This value needs to be aligned with application name as used in AV.
ShowSeriesSelector	Specifies whether the Study/Series Selector window appears before launching the AV application. Accepted values are true or false, where: • True displays the selector window, allowing users to choose additional studies or series before the AV application launches. • False bypasses the selector window and launches the AV application directly.
applicationId	This parameter is a static configuration value and must always be set to pacs_plugin.

300018593821_A/881 * 2026-09-10

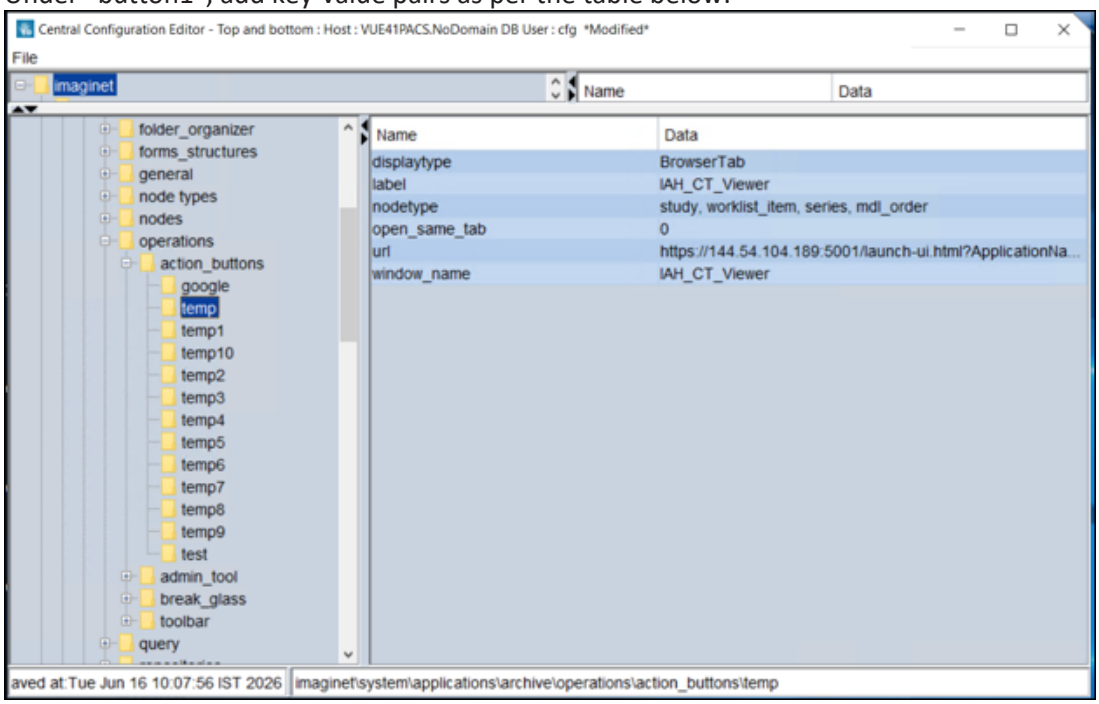
Ex: Command : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --kiosk --start-minmized "https://dicomgateway:5001/launch-ui.html?ApplicationName=MR Cardiac Suite&StudyUID=@STUDY_INSTANCE_UID@&StudyLevelApps=true&ShowSeriesSelector="false "&applicationId=pacs_plugin"

NOTE

You can also configure applications from **Application Setting > Report & 3rd party integrations >Action Buttons Settings in Vue Client**.

From the patient jacket

1. 1. Log on to the Vue PACS server.
2. Open the Central Configuration editor, go to imaginet\system\applications\archieve\operations\action_buttons.
3. There is a key for each action button. The format for each key is “buttonX”, where X is a number used to determine the Action Button position in the Action Buttons list in the application.
4. Under “button1”, add key-value pairs as per the table below:



Repeat these steps for all the applications that need to be configured.

Attribute	Value	Comments
displaytype	BrowserTab	The application where we would like to embed-in.
label	Application Name	User-defined name

300018593821_A/881 * 2026-09-10

Philips

Attribute	Value	Comments
url	https:// hscadapter_baseurl:5001/ launch-ui.html? ApplicationName=app_name&Study UID=@study_instance_uid@&ShowS eriesSelector="false"&applicationId= pacs_plugin"	Launch URL for the application
window_name	Application Name	User-defined name

Command Parameter Name	Comments
hscadapter_baseurl	URL of the service endpoint URL used for accessing the AV application. Use the hostname or fully qualified domain name (FQDN) of the gateway system if it is deployed on premises. For cloud deployments, use the service URL provided by the operations team.
StudyUID	Mandatory, the value should always be set as @ study_instance_uid @. During application launch, this placeholder is automatically replaced with the UID of the selected study.
ApplicationName	Name of the AV application. This value need to be aligned with application name as used in AV.
ShowSeriesSelector	Specifies whether the Study/Series Selector window appears before launching the AV application. Accepted values are true or false, where: • True displays the selector window, allowing users to choose additional studies or series before the AV application launches. • False bypasses the selector window and launches the AV application directly.
applicationId	This parameter is a static configuration value, and must always be set to pacs_plugin.

Ex URL: https://dicomgateway:5001/:5001/launch-ui.html?ApplicationName=MR Cardiac Suite&StudyUID=@study_instance_uid@&ShowSeriesSelector="false"&applicationId=pacs_plugin

Accept Reject Tool Configuration for Third-Party AI Applications

This section described how to embed third-party AI applications within the PACS Diagnostic Viewer. There are two options:

300018593821_A/881 * 2026-09-10

1. **Accept/reject tool is embedded within the patient jacket**: For PACS versions >= 12.2.8.X, the accept/reject tool is suggested to be embedded within the Patient Jacket as an external web application.
2. **Accept/Reject tool within the Diagnostic Viewer**: The sites that do not have Vue Explorer, and only archive explorer, can go with this option where the accept/reject tool is embedded in the diagnostic viewer.

Accept/Reject tool within Patient Jacket

Below are the steps to configure accept/reject tool as external application in the patient jacket:

1. Open the Central Configuration editor, Go to imaginet\system\applications\mediprime\integrations\action_buttons
2. There is a key for each action button. The format for each key is “buttonX”, where X is a number used to determine the Action Button position in the Action Buttons list in the application. For example, adding the action button “button1” will appear as the first tab on the patient jacket viewer.
3. Under “button1”, add key-value pairs as per the table below:

Attribute	Value	Comments
applications	patient_jacket	The application where we would like to embed-in.
name	1	Name of the tool
auth_token_required	1	Disabled – No Single Sign-On. Enabled – Single Sign-On using SHS. More on this is described in upcoming section Single Sign-On.
open_on_start_session	1	Enabled. Indicates accept/reject tool loads upon opening of the patient jacket.
open_only_by_condition	1	Enabled. Indicates opening of the accept/reject tool upon a condition mentioned at start_session_activation_condition attribute (below).
text	AI Result Viewer	Name of accept/reject tool that appears for the user
url	https:// ARTProxy_baseurl:5002/ study?requestType=STUDY &studyUID=@study_instance_uid@ @authentication@	URL to open along with StudyID context

300018593821_A/881 * 2026-09-10

Attribute	Value	Comments
start_session_activation_condition	@tamar_misc_string_6@ @in@ @Pending@ @and@ @tamar_study_status@ @not equal@ @READ@	Condition on which the accept/reject tool activates
OPTIONAL: auto_focus	1	Enabled. Upon opening of the patient jacket, the user is on the accept/reject tab.

NOTE

ARTProxy_baseurl in the URL parameter is the host /domain name where the Accept Reject Tool proxy is running. This changes according to site-specific deployment.

Accept/Reject tool within Diagnostic Viewer

Below are the steps to configure the accept/reject tool as an external application in the Diagnostic Viewer:

1. Open the Central Configuration editor, go to imaginet\system\applications\mediprime\integrations\action_buttons
2. There is a key for each action button. The format for each key is “buttonX”, where X is a number used to determine the Action Button position in the Action Buttons list in the application. For example, if you add the action button “button1”, it appears as the first tab in the diagnostic viewer.
3. Under “button1”, add key-value pairs as per the table below:

Attribute		
applications	mediprime	The application where we would like to embed-in.
name	Accept_Reject_Tool	Name of the tool
open_on_start_session	1	Enabled. Indicates the accept/reject tool loads upon opening the diagnostic viewer.
text	AI Result Viewer	Name of the accept/reject tool that appears for the user.
url	https:// ARTProxy_baseurl:5002/ study?requestType=STUDY &studyUID=@study_instance_uid@ @authentication@	URL to open along with StudyID context.
OPTIONAL: auto_focus	1	Enabled. Upon opening the Diagnostic Viewer, the user is on the accept/reject tab.

300018593821_A/881 * 2026-09-10

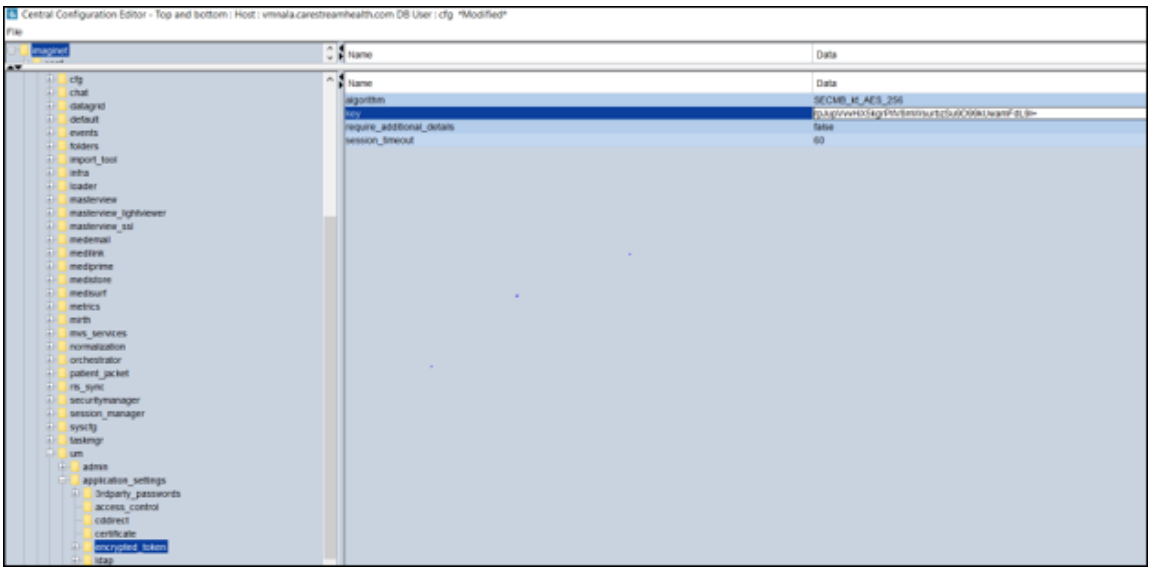
NOTE

ARTProxy_baseurl in the URL parameter is the service endpoint URL used for accessing the Accept/Reject tool. Use the hostname or fully qualified domain name (FQDN) of the gateway system. This changes according to site-specific deployment.

Single Sign-On

Single sign-on is achieved via the option for symmetric key encryption that Vue PACS supports and aligns with the Advance Image Insights Solution. The Accept/Reject tool can either be embedded within patient jacket or the Diagnostic viewer. It is recommended to embed it in the patient jacket, however it is per customer preference to choose either patient jacket or Diagnostic viewer.

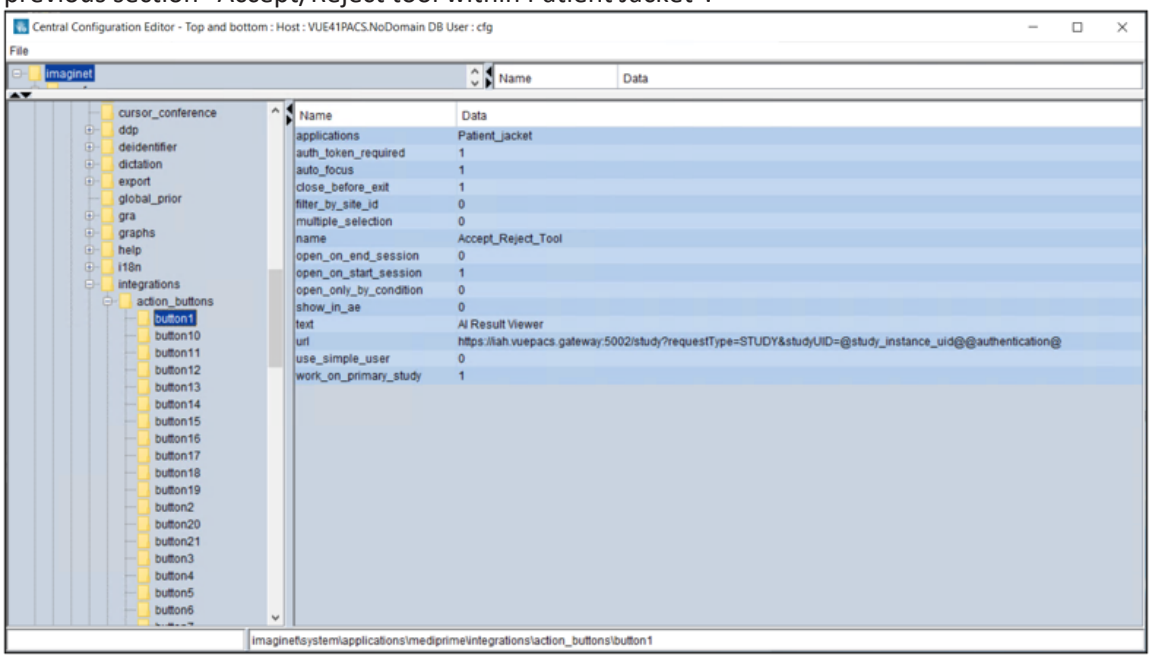
Make sure you have configured the symmetric shared key at system\applications\um\application_settings\encrypted_token\key. There are other details as shown in the screenshot below.



Accept/Reject Tool in Patient Jacket with Single Sign On (SSO)

300018593821_A/881 * 2026-09-10

Make sure you have SSO enabled for the accept/reject tool, as described in configuration of the previous section "Accept/Reject tool within Patient Jacket".



SSO Features and Limitations

1. The session timeout validation of SSO needs to be configured on the Advance Image Insights Solution side. It is suggested to keep it at 5 minutes so that the token becomes invalid after 5 minutes.
2. For the diagnostic viewer, we cannot have conditional opening, i.e we cannot configure to open the accept/reject tool based on a condition like status=Pending. Hence, once configured, third-party AI applications are always available in the diagnostic viewer
3. Accept/Reject tool SSO for Diagnostic viewers can only be used at sites where all users are in same time zone. This is because currently, Diagnostic viewer does not support embedding time zone within the token, unlike Patient Jacket implementation
4. We cannot have Accept/Reject tool in the patient jacket and diagnostic viewer at the same time. Either one of them is allowed.

Configuration for the applications in ISPACS

Prerequisites: The following details should be available

- URL for the BART and AV
- Secret Key

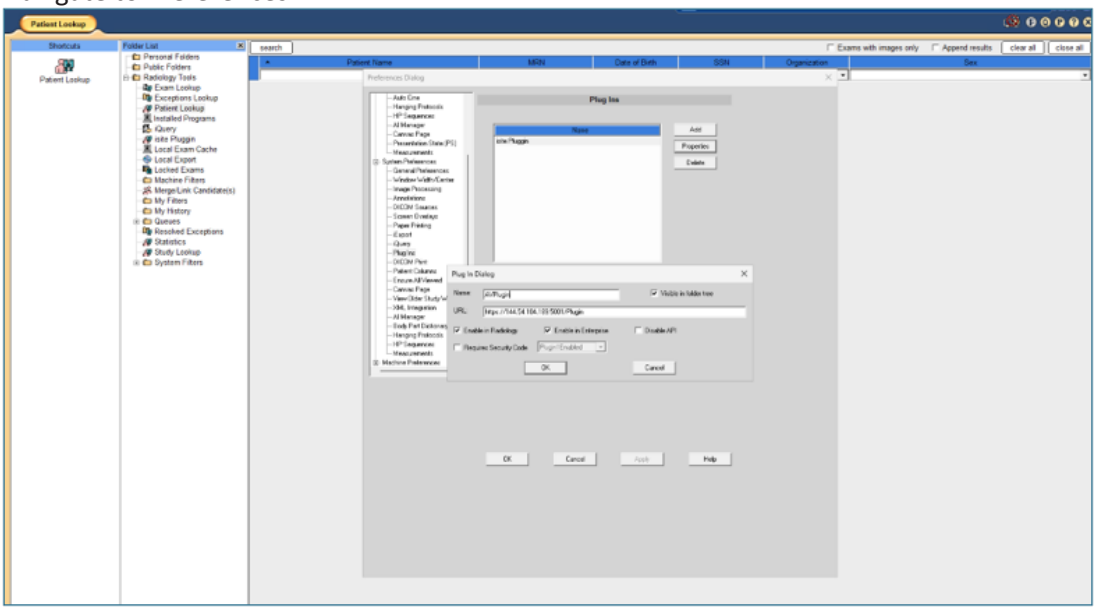
Advanced Visualization (AV) applications

This section outlines the instructions required for configuring the plugin required for AV applications.

1. Log in to IS-PACS using an account with administrative privileges.

300018593821_A/881 * 2026-09-10

2. Navigate to Preferences



3. Open either **Machine Preferences** or **System Preferences**, depending on where you want to configure the plugin.
4. Select the section **Plugin In**.
5. Select **Add** to create a new plugin configuration, and in the dialog specify the Name and URL as follows:
   - **Name** -- Type a name for the plugin (for example, AVPlugin).
   - **URL** -- Type a URL in the following format: https://<HSCAdapter_BaseURL>:5001/Plugin/<Token>
     Where "HSCAdapter_BaseURL" is the service endpoint URL for accessing the AV application; use either the hostname or fully qualified domain name (FQDN) of the gateway system; and
     "Token" is used to authenticate and authorize access to the plugin. The token is configured as part of the deployment process and is provided by the service team.
   - Under the plugin options, select only the checkboxes **Enable in Radiology** and **Enable in Enterprise**. Ensure that all other checkboxes are clear.
6. Select **OK** to save the plugin configuration.
7. On the Preferences dialog, select **OK** again to apply the changes.
8. Restart the IS-PACS client for the configuration changes to take effect.

Accept/Reject Tool Configuration (Third-Party AI Applications)

This section outlines the instructions required for a installing third-party AI applications' plugin on a client machine, and configure its settings on the ISPACS. This is required to launch the Accept/Reject Review tool in ISPACS, which can be used to View and Accept / Reject AI results available for an exam.

Prerequisites

300018593821_A/881 * 2026-09-10

- ISR 4.7.62.0 in Client Machine
- UDM 3.1.53.0

Standalone Manual Installation



The third-party AI applications' plugin build consists of two installers:

- AIManagerPluginSetup.msi
- Setup.exe

Double-click **setup.exe**. It launches the installation wizard. Follow the steps mentioned in the wizard.

Post-Installation Configuration

After the third-party AI applications' plugin installation, users need to launch IntelliSpace Radiology to configure certain Preferences.

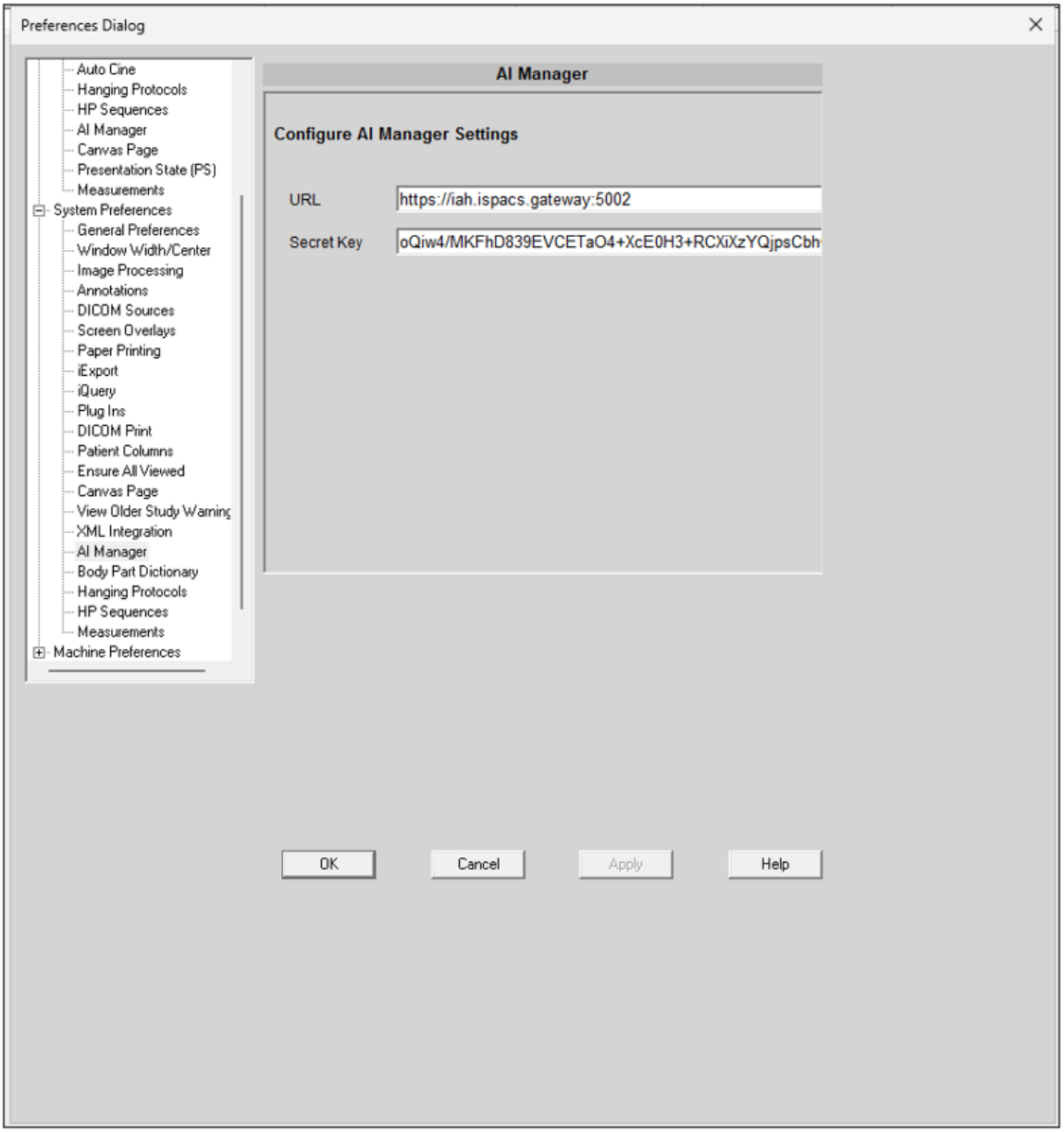
Navigate to **Preferences > System Preferences > AI Manager Preference Administrator** to configure the URL for the Accept/Reject tool under AI Manager URL configuration and the Secret Key.

NOTE

The below values are provided by the Philips service team.

URL (URL pointing to ART Proxy in format https://ARTProxy_baseurl:5002)
Secret Key (AES256 key encoded as BASE64). This value needs to be aligned with the third-party AI applications.

300018593821_A/881 * 2026-09-10



- Navigate to **Preferences > User Preferences > AI Manager**. You can configure Auto Launch of the AI Manager tool when canvas page of study is opened.

NOTE

Any changes to User and System preference requires a restart of IntelliSpace Radiology for the changes to take effect.

300018593821_A/881 * 2026-09-10

Philips

4 Relevancy Definition

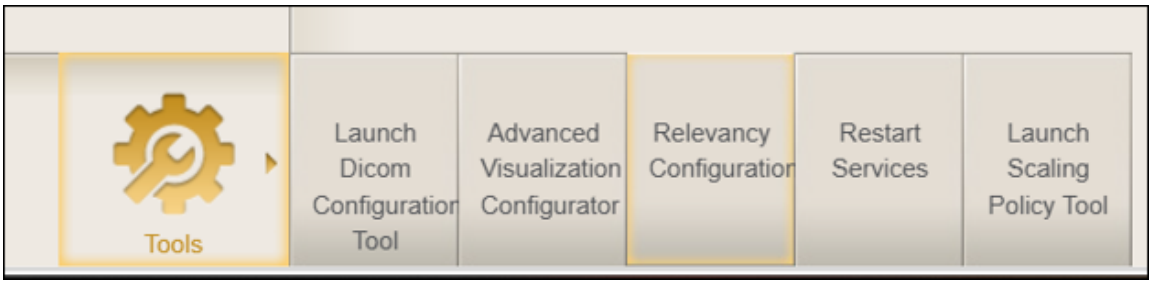
Relevancy rules definition for AI applications

Relevancy rules for AI applications are defined in alignment with site-specific requirements on the AII Solution, as part of customer onboarding and configuration.

Relevancy rules definition for AV applications

Login to AVW management tool using Appstream client with one of the following URLs:

- For Concerto: <customer base URL>/appstream/stream-urls?ApplicationId=CMT
  Login with provided domain credentials. Note that once domain credentials expires, contact Philips support for password reset.
  On the Dashboard screen, select one of the AVW servers and select **Manage** to launch the AVW management tool.
- For AVW Server: <customer base URL>/appstream/stream-urls?ApplicationId=PMTLauncher
  Login to AVW management tool using admin-provided credentials. Navigate to **Tools** > **Relevancy Configurator**



Log in with provided IAH credentials (HSP IAM).
Follow the AVW System Admin guide for rules configuration.

300018593821_A/881 * 2026-09-10

300018593821_A/881 * 2026-09-10

Philips

5 Audit

Prerequisites The user must have access to the Audit Viewer. Note that this URL varies depending on the deployment region, and is provided by the Philips Service team.

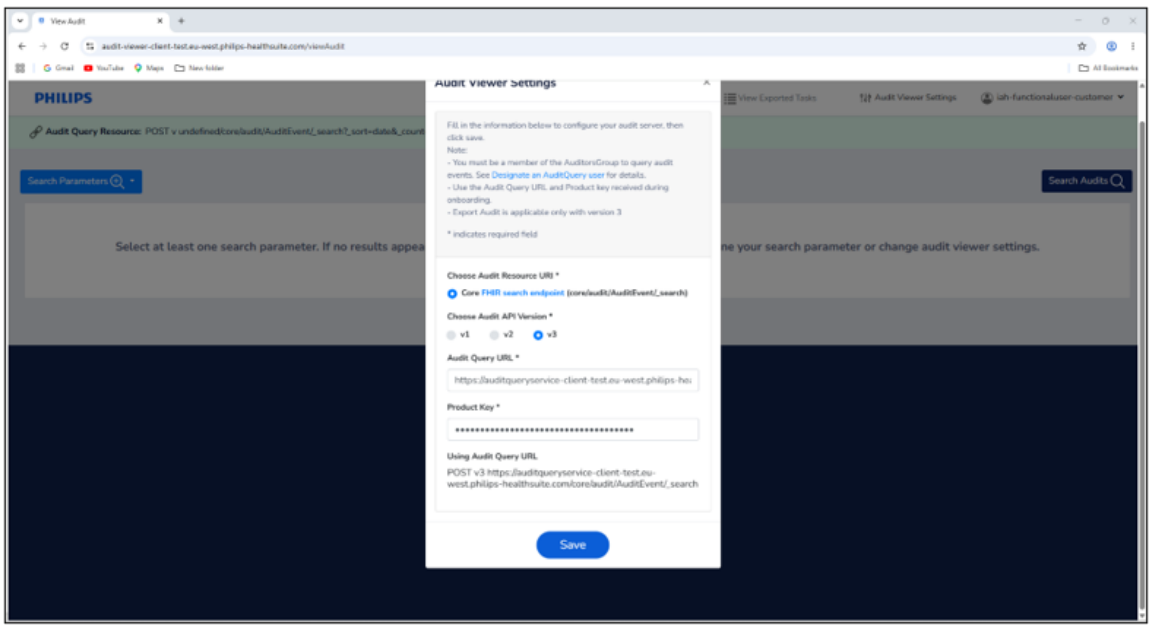
How to view audit logs

How to log in

1. Open the Audit Self-Service Event Viewer using one of the URLs above for the environment and region you are working on.
2. Select the **Log In** button on the upper right-hand corner.
3. The HSDP IAM login screen appears. Enter the required IAM credentials. Note that the IAM account should be a member of the Group with AUDIT.READ (for log view) and AUDIT.EXPORT (for export) permission.
4. The audit server screen appears. Enter the audit service Query Name and Product Key. See below for more information.

Configure the audit server settings

Once login is done, enter the Audit Query URL and Product Key provided by the Philips Service team, then select **Save**.



How to search

Once you logged into the Audit Self-Service Event Viewer, you can select one or more search parameters from the **Search Parameters** dropdown list. You can search within the parameters to choose the right one.

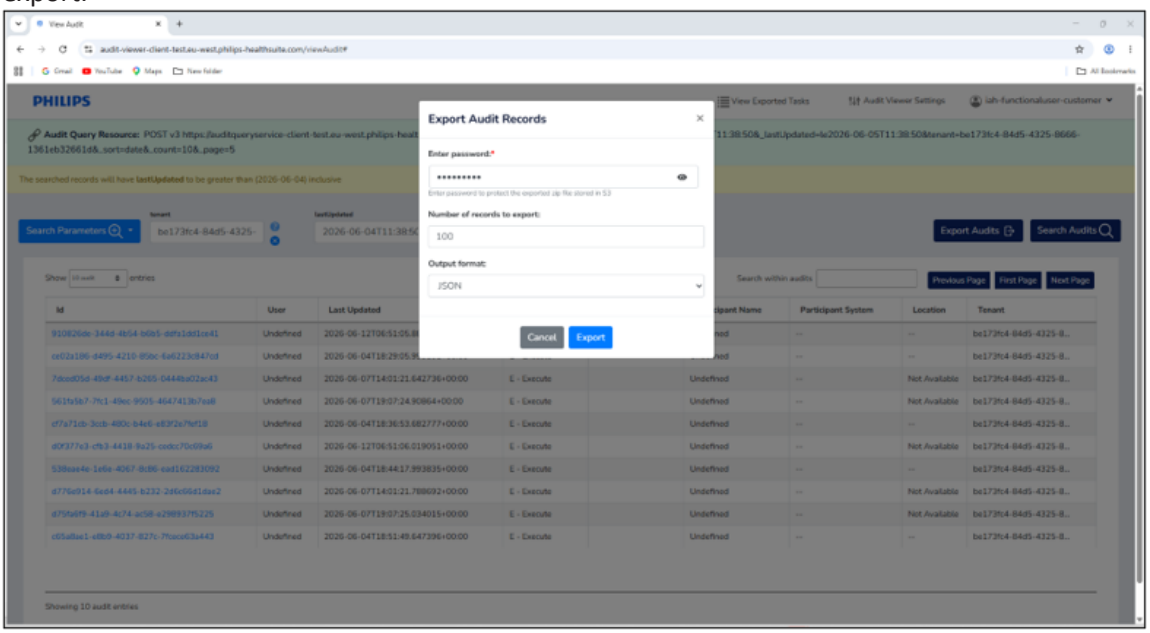
Search results are based on the selected search parameters.

Specify the search parameters, then select **Search Audits** to view the logs.

300018593821_A/881 * 2026-09-10

How to export Audit logs

To export the logs, select **Export Audits** and enter the password and number of records to export.



Export jobs can be found under **View Exported Tasks**. Once an export job is complete, the resulting ZIP file can be downloaded and extracted using 7z tools.

3000185938 21_A/881 * 2026-09-10

6 AIO Configuration

This section describes the creation and editing of the site resources for example: the DICOM gateway, device, delivery nodes, query retrieve node, HL7 client, and Site Config definition and configuration.

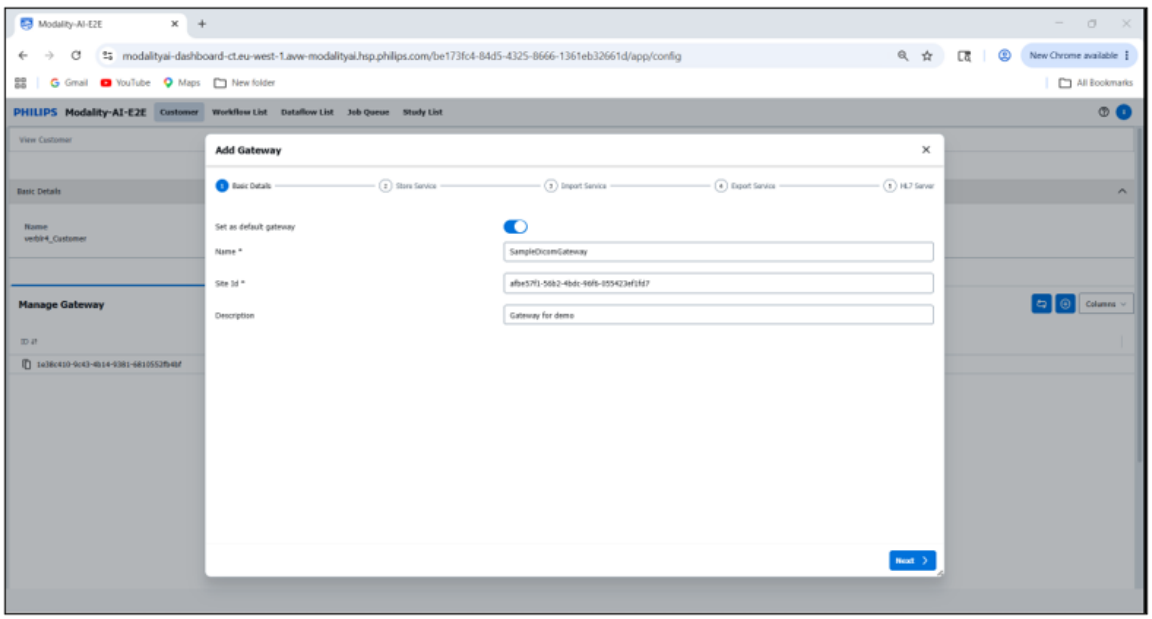
Prerequisites:

- Access to the modality dashboard for the customer ORG.
- Device service account details: device_svc_acc
- Certificate details (if a secure connection is enabled for store, import, export and HL7 services in DICOM gateway.
- Configuration must be performed by a user who is part of the gateway resource groups in the customer (proxy) organization under the IAH root organization.

To start: Log into the Modality Dashboard UI for the customer. This URL is provided by the Philips Service team.

DICOM gateway configuration

To modify the DICOM gateway configuration, select the Gateway tab, select the gateway, then press the button **Edit** to edit the gateway.



Update the basic details:

- **Set as default gateway**: Mandatory, specify one of the gateways as the default to retrieve device/site configurations for exporting or querying.
- **Name**: Mandatory field, specify a readable name for the gateway.
- **Site Id**: Mandatory field, specify the UUID of the site organization created for the site under the customer (proxy) organization in IAM.

300018593821_A/881 * 2026-09-10

- **Description**: Description for the gateway

Press **Next**.

Store service configuration (configurations for Store service, for receiving the data from remote devices)

Update the configuration for the Store service as outlined below:

- **Network Settings**: Store service port (default 11112). This value is defined in the env file defined for gateway
- **Advanced Settings** Use the default value as defined below:
  - **PDU Length**: Defines the maximum amount of DICOM protocol data that can be transmitted within a single Protocol Data Unit (PDU) over a TCP connection. A recommended value is 65,535 bytes.
  - **ARTIM Timeout (in seconds)**: Specifies the maximum timeout period for waiting on association-related DICOM protocol events, such as Association Request, Association Reject, and Association Release. The recommended timeout value is 3000 milliseconds.
  - **Association Idle Timeout (in seconds)**: Specifies the maximum period an association can remain inactive before it is automatically closed. The default value is 4500 milliseconds.
  - **Enable Secure Connection** This step is optional and should be performed once the certificate is available. If the certificate is not available at this stage, revisit this step later. Enable a secured connection if communication between devices sending data and the DICOM gateway must be secured. When enabled, the DICOM gateway's store service presents a certificate to the client device, upon receiving a connection request for data ingestion.

    For detials, see the upcoming section "To configure and use secured communication for store service".
  - **Service Configuration**: Mandatory field, define multiple service configurations corresponding to different AE titles that are configured in gateway to receive the data
  - **AE Title**: Mandatory field, specify an AE title for the DICOM gateway node
  - **IAM Organization ID**: Mandatory field, specify the UUID of the customer (proxy) IAM organization under which the gateway is defined.
    Note that if both AV and AI are enabled, then both organizations must be mapped.
  - **Allow Any**: Keep this deactivated, to prevent data from being sent to the gateway by unknown devices.
  - **Enable DeIdentification**: Enable this option if data needs to be de-identified for the specified AE title.
    Note that for AV data organization, De-identification is not applied, and this option must remain deactivated. For AI data organization, De-identification is applied, and this option must remain enabled.
  - **Enable Filter**: Enabled always. Data is filtered before transferring to the DICOM store.

To configure and use secured communication for store service

1. Open the corresponding gateway configuration and enable secure communication for the store service.

300018593821_A/881 * 2026-09-10

2. Select the required TLS version. TLS 1.0 or higher ensures maximum interoperability, while TLS 1.2 provides maximum security.
3. Provide certificate details. The UI allows uploading the certificate along with its name, display value, and password. This certificate is presented to the client when a C STORE request is received. Both self-signed certificates and certificates issued by a trusted Certificate Authority (CA) can be used. The certificate must be in .p12 or .pfx format. In case a self-signed certificate needs to be used, the DICOM Gateway installation script allows generation of the certificate.
4. Press **Next**.

Import service configuration (configurations for import service, for retrieving data from a remote device)

Add or update the configuration for import service, as described below:

- **Name**: Mandatory field, specify a readable name for the import service
- **Description**: Additional details
- **AE Title**: Mandatory field, specify the AE title of the import service of the DICOM Gateway
- **Data Organizations**: Mandatory field, specify the UUID of the customer (proxy) IAM organization under which the gateway is defined. Map all IAM organizations that are configured under this gateway and require import to be supported.

Press **Next**.

Export service configuration (configurations for export service, to export data to a remote devices)

Add or update the configuration for import service, as described below:

- **Name**: Mandatory field, specify a readable name for the export service
- **Description**: Additional details
- **AE Title**: Mandatory field, specify the AE title that the export service identifies with
- **Data Organizations**: Mandatory fields, specify the UUID of the customer (proxy) IAM organization under which the gateway is defined. Map all IAM organizations that are configured under this gateway and require export to be supported.

Press **Next**.

HL7 server details

This step is required if AI is enabled for the customer.
These are configurations for the HL7 service to export HL7 data to remote devices. Add or update the configuration for HL7 server as described below:

- **Enable HL7**: If HL7 configuration is required
- **Data organization ID**: Mandatory field, specify the UUID of AI customer (proxy) IAM organization
- **Receiving Application**: Mandatory field, should match the HL7 client's Receiving Application, as it is used to identify the appropriate workflow on the HL7 server

300018593821_A/881 * 2026-09-10

Philips

- **Sending Application**: Mandatory field, the software or system sending the message, e.g., Gateway. This value goes in the message header of the outgoing HL7 message as the sending application, per standard. Note that this value needs to align with the expected value at the PACS system, e.g., ISPACS always expects this value as AIManager.
- **Sending Facility**: The organization sending the message. This value goes in the message header in the outgoing HL7 message as the sending facility, per standard.
- **De-ID**: Always enabled

Enable secure connection (for Import, Export and HL7 server)

This step is optional and should be performed once the certificate is available. If the certificate is not available at this stage, revisit this step later. When secure communication is enabled on a destination, e.g., PACS or Modality, the gateway services, i.e Export, Import, and HL7 Forwarder services, must be configured for secure communication.

To accomplish this, enable secure connection in each of the service configurations. Once enabled, the DICOM gateway services uses the TLS to request the server's certificate when connecting. It then authenticates the destination server and encrypts all communications.

Certificate requirements

Gateway services require certificate details to operate securely. Certificates may be self-signed or issued by a trusted Certificate Authority (CA). If the certificate is not issued by a trusted CA, it must be manually installed in the trusted root certificate store on the gateway system.

If installation of the certificate into the trusted root certificate store is not feasible, the certificate can instead be configured within the gateway service configuration. In case a self-signed certificate needs to be used, the DICOM Gateway installation script allows generation of the certificate.

Steps to Configure TLS for Gateway Services

Open the corresponding gateway configuration and enable secure communication for the service. Select the required TLS version. TLS 1.0 or higher ensures maximum interoperability, while TLS 1.2 provides maximum security.
Provide certificate details. The UI allows uploading the certificate along with its name and display value, which is required only if the certificate is not installed into the trusted root certificate store. The certificate must be in .p12 or .pfx format for HL7 Server, and .cer format for import and export service.

Device configuration

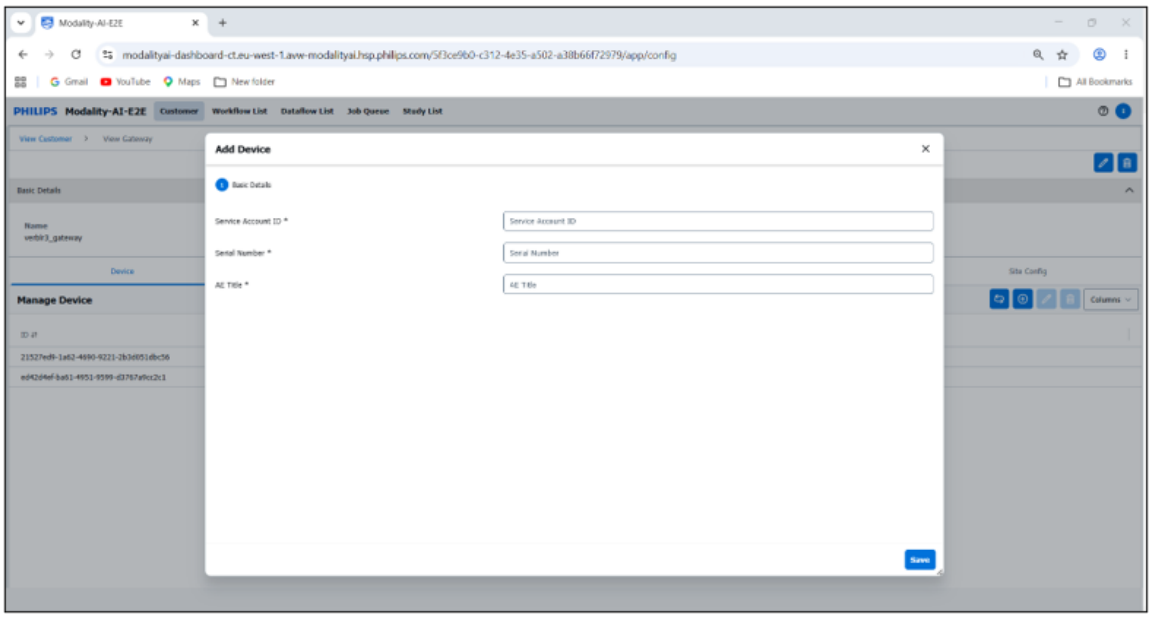
Register each point-of-care device that is configured to send data to the DICOM gateway. On the created DICOM Gateway, navigate to the **Device** tab and select **Add** to enter device details as described below.
If the device is already present and needs to be edited on the created DICOM Gateway, navigate to the **Device** tab, then select a device and select **Edit**.

Basic details

- **Service Account ID**: Mandatory field, specify the service account created for the device (device_svc_acc) in the customer (proxy) organization in IAM.
- **Serial Number**: Mandatory field, user-defined identifier for the device

300018593821_A/881 * 2026-09-10

- **AE Title**: Mandatory field, specify the AE title the device is registered with, e.g., PACS AETitle: ORTHANC. Once details are added, press **Save**.



Delivery destination configuration

The details of the remote devices, i.e PACS systems, where application results need to be transferred, needs to be registered. On the created DICOM gateway, select the **Delivery Destination** tab. Select **Add** to enter the details of the remote device. If the delivery destination is already present and needs to be edited on the created DICOM Gateway, navigate to the **Delivery Destination** tab, select the device, then press **Edit**.

Add or update the configuration for devices as described below

DICOM details

Add all the destination node details:

- **AE Title**: Mandatory field; specify AE title of the remote device
- **Port**: Mandatory field; specify port number that the device is configured to use
- **Host Name**: Mandatory field; specify hostname of the system where remote device is installed
- **IP Address**: Mandatory field; specify IP address of the system where remote device is installed
- **Network Timeout (in seconds)**: Mandatory field; specify values as 3600
- **Advanced Settings**: Mandatory fields; use the default values as defined below
  - **PDU Length**: Defines the maximum amount of DICOM protocol data that can be transmitted within a single Protocol Data Unit (PDU) over a TCP connection. A recommended value is 65,535 bytes.

300018593821_A/881 * 2026-09-10

  - **ARTIM Timeout (in seconds)**: Specifies the maximum timeout period for waiting on association-related DICOM protocol events, such as Association Request, Association Reject, and Association Release. The recommended timeout value is 3000 milliseconds.
  - **Association Idle Timeout (in seconds)**: Specifies the maximum period an association can remain inactive before it is automatically closed. The default value is 4500 milliseconds.

Node configuration for query retrievals

Define the details of the remote devices where the gateway can query and retrieve the priors' studies required by applications. On the created DICOM gateway, select the **Query Retrieve Node** tab. Press **Add** to enter the details of the remote device to be used for query retrievals. If the Query Retrieve node is already present and needs to be edited on the created DICOM Gateway, navigate to the **Query Retrieve Node** tab, select device, then press **Edit**. Add or update the configuration for devices as described below:

Basic details

- **Name**: Mandatory field, specify a user-defined name for the destination node
- **Type**: Keep as DICOM

DICOM details

Add all the following Query node details:

- **AE Title**: Mandatory field, specify the AE title of the remote device
- **Port**: Mandatory field, specify the port number that the device is configured to use
- **Host Name**: Mandatory field, specify the hostname of the system where remote device is installed
- **IP Address**: Mandatory field, specify the IP address of the system where remote device is installed
- **Network Timeout (in seconds)**: Mandatory field, specify values as 3600
- **Advanced Settings**: Mandatory fields, use the default values as defined below:
  - **PDU Length**: Defines the maximum amount of DICOM protocol data that can be transmitted within a single Protocol Data Unit (PDU) over a TCP connection. A recommended value is 65,535 bytes.
  - **ARTIM Timeout (in seconds)**: Specifies the maximum timeout period for waiting on association-related DICOM protocol events, such as Association Request, Association Reject, and Association Release. The recommended timeout value is 3000 milliseconds.
  - **Association Idle Timeout (in seconds)**: Specifies the maximum period an association can remain inactive before it is automatically closed. The default value is 4500 milliseconds.

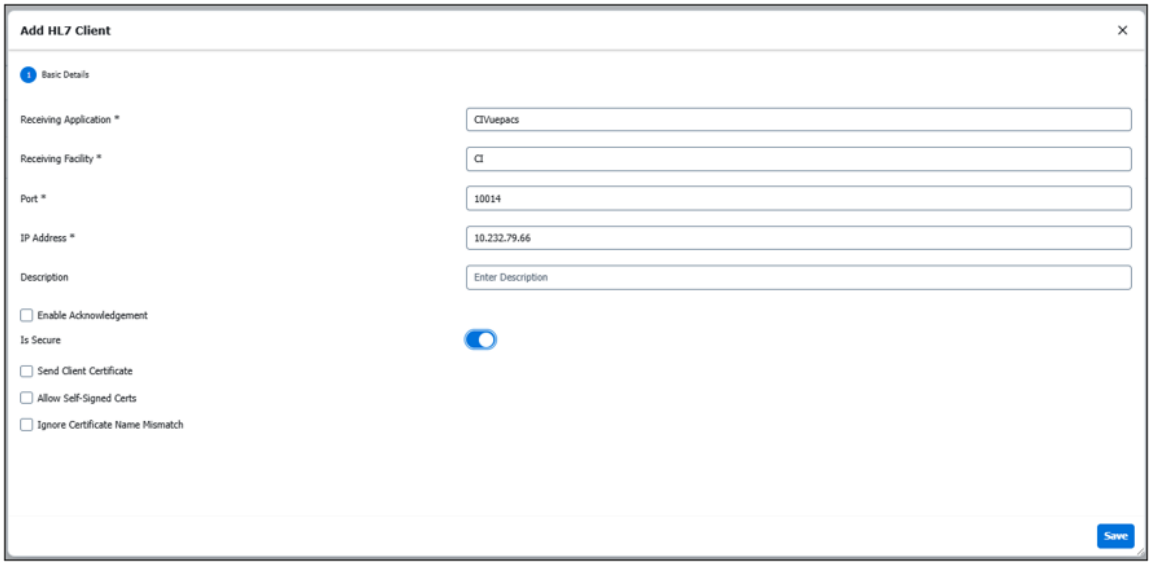
HL7 client configuration

Define the details of the device (PACS) system where the gateway can send HL7 message generated by the apps.
On the created DICOM gateway, select the HL7 client tab. Select **Add** to enter the details of the device to be used to send the HL7 message. The dialog **Add HL7 Client** opens

300018593821_A/881 * 2026-09-10

If the HL7 client configuration is already present and needs to be edited on the created DICOM Gateway, navigate to the HL7 client tab, select configuration, then select **Edit**. Add or update the configuration as described below:

Basic details



- **Receiving Application**: Mandatory field, specify the identifier of the target system receiving HL7. This value goes on the message header of the outgoing HL7 message, per standard.
- **Receiving Facility**: Mandatory field, identifier of the organization where the receiving system is hosted. This value goes on the message header of the outgoing HL7 message, per standard. Note that this value needs to align with the expected value at the PACS system. E.g., ISPACS always expects this value to be "AIManager".
- **Port**: Mandatory field, specify the port address of the device accepting the HL7 message
- **IP Address**: Mandatory field, specify the IP Address of the system where the device is installed
- **Enable Acknowledgment**: Flag to indicate the server sends acknowledgment.
- **Is Secure**: Flag to indicate secure communication. Enable this flag if the PACS system supports secure connection.
- **Send Client Certificate**: Control whether or not the client's certificate is sent to the server, enabling client authentication to occur, as well. If mutual authentication is enabled, the client certificate should be configured in the HL7 server resource.
- **Allow Self-Signed Certs**: Flag to indicate whether certificate validation should be bypassed.
- This setting **allowSelfSignedCert=true** is not recommended for production environments. It deactivates validation of the certificate chain, and may allow connections using untrusted, expired, revoked, or malicious certificates. Use it only in development or controlled testing environments.
- **Ignore Certificate Name Mismatch**: Control whether to ignore mismatch errors in the certificate name.

300018593821_A/881 * 2026-09-10

Philips

Site configuration



After the delivery destination and query retrieve node are defined, define the site configuration to indicate how application results are delivered, and the default query retrieve node.
On the **Import Config** tab, select the default query retrieve node to import the priors' studies requested by the applications.

In the **Export Config** tab, the delivery destinations define the following supported configurations:

- **Default Delivery Destination**: default destination where application results will be transferred from, if no other configuration is defined.
- **Application to Delivery Destination**: Application-specific configuration to define where the transfer of application-specific results should occur.
- **Export to Source**: Results are transferred back to the source device from where data was sent. When **Export to Source** is enabled, define device-to-delivery destination mapping.

The order of precedence of the used configuration is:

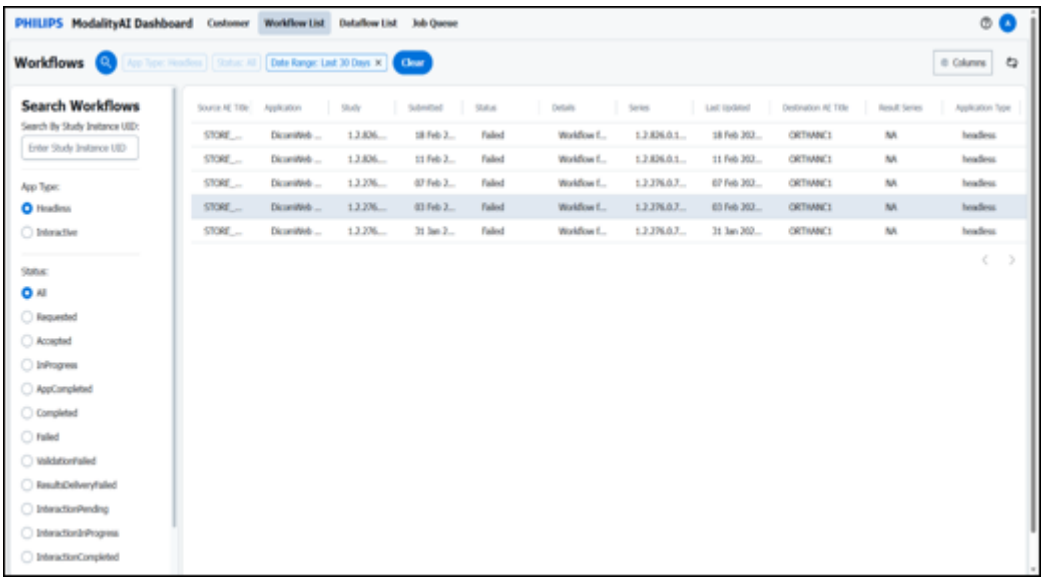
1. Application to Delivery Destination
2. Export to Source
3. This Default Delivery Destination

300018593821_A/881 * 2026-09-10

7 Monitoring the workflow (data and application) via dashboard

This section discusses how to use the Admin Dashboard to track workflow, dataflow, data ingestion, and export status and details. Access to the Admin Dashboard is provided during onboarding.

Tracking Workflows



Workflows are triggered from a registered device for a subscribed application for the selected data. You can identify each workflow based on its unique ID.
Once a workflow is successfully triggered, you can track it on the **Workflow List** tab of the Admin Dashboard. By default, the Admin Dashboard provides details about the following:

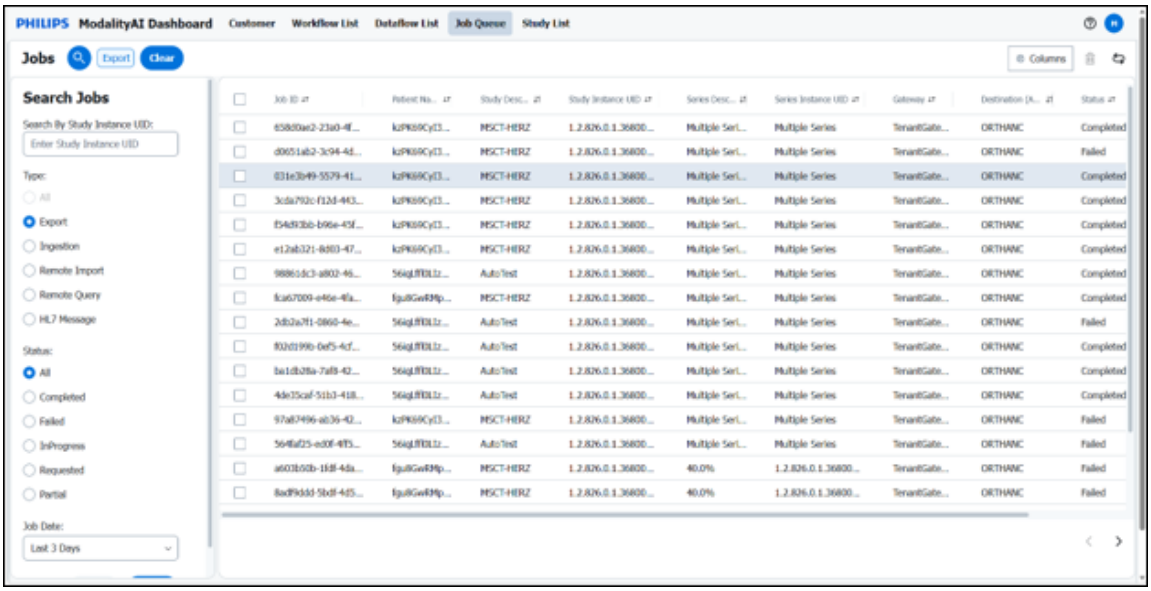
- **Source AE Title** - AE title of the device that triggered the workflow.
- **Application** - Name of the application on which the workflow is triggered.
- **Study** - Study instance UID of the input study.
- **Status** - Current status of each workflow.
- **Destination AE Title** - AE of the delivery destination where results are transferred, if configured.
- **Submitted** - Date and time when this workflow was triggered.

NOTE

Use the "Search" icon to filter workflows by Study Instance UID, status, and date. If you select the workflow, you can see all the related jobs (export, remote query, remote import and HL7) in a dialog.

300018593821_A/881 * 2026-09-10

Tracking jobs

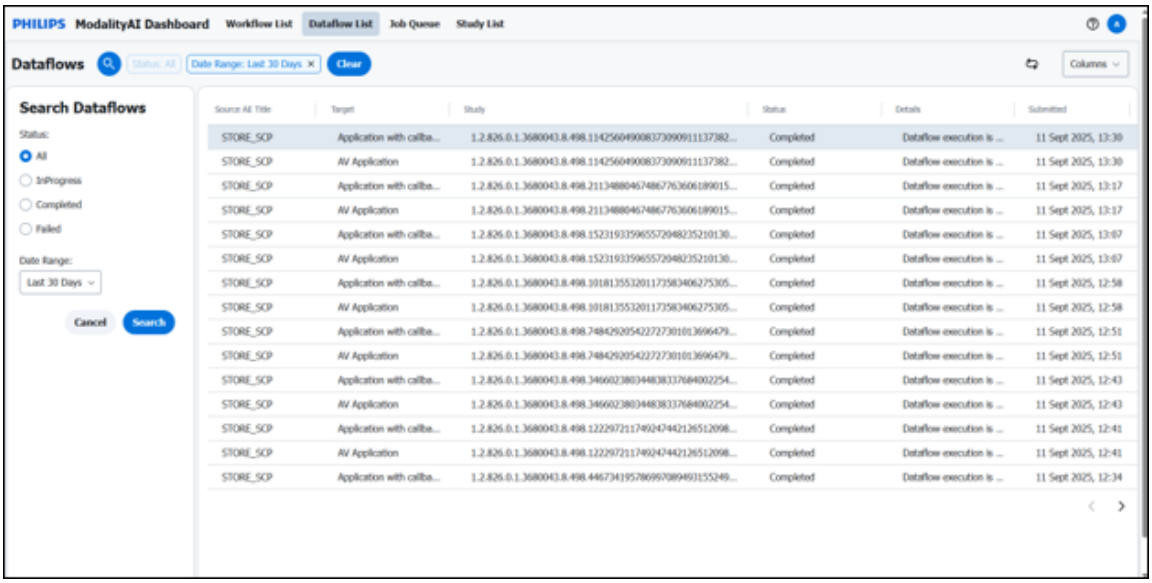


Each workflow includes multiple DICOM data transfers: one for transferring input data from PACS/Modality systems to the AI application, and others for transferring the results from the AI application to the PACS/Modality.
The Admin Dashboard provides a Job Queue screen where you can track each data transfer. You can track the following job types on this screen:

- **Ingestion** jobs - track the input of the data transfers from PACS to the DICOM Store, and the results of the data transfers from the AI application to DICOM Store.
- **Export** jobs - track the results of data transfers from the DICOM Store to the PACS.
- **Remote Query** jobs - track query of the studies from remote nodes
- **Remote Import** jobs - track the transfer of studies from remote nodes
- **HL7 Message** jobs - track HL7 messages like priority update and study status to the remote nodes

300018593821_A/881 * 2026-09-10

Tracking dataflows



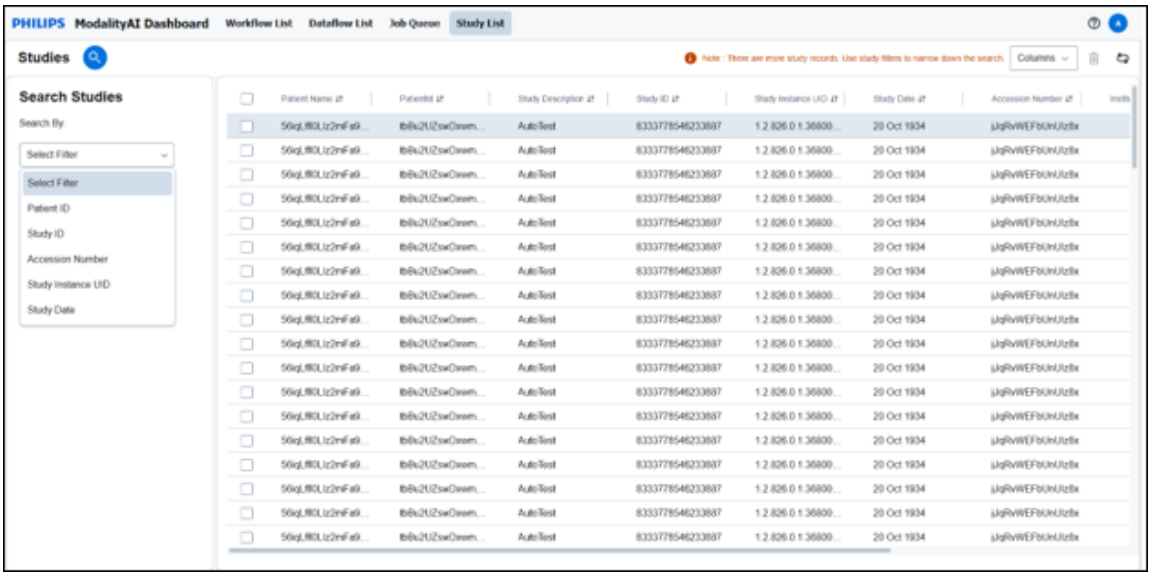
Data is transferred to the relevant applications as soon as they are sent from the PACS system to the DICOM Gateway, and then to DICOM Store.
These data transfers from the DICOM Store service to applications are called dataflows. You can track each dataflow on the **Dataflow List** tab.

- **Source AE Title** - AE title of the device that sent the data
- **Study** - Study instance UID of the input study
- **Status** - Current status of each data transfer
- **Details** - Details of the data transfer
- **Submitted** - Date and time when this workflow was triggered

You can also configure the columns on the Dataflow List and reorder them. Your selected column order is retained for future sessions.
Use the "Search" icon to filter dataflows by study Instance UID, status, and date.

300018593821_A/881 * 2026-09-10

Study List



The Study List tab shows the data that is ingested in the DICOM Store. You can select a study to view the series within the study, and then select an individual series to view its metadata. Use the **Delete** button to delete the selected studies.

NOTE

This is a hard delete. Once a study is deleted, the operation cannot be undone.

Correlating the data

- A study sent from PACS to a DICOM Gateway is sent to the DICOM Store. Once the study is uploaded to the cloud, it can be tracked in the **Job Queue**. Each ingestion job typically represents a series in a study, but it may also represent a part of the series.
- Once the **Job Queue** shows that the data is successfully ingested, the data is sent to the relevant applications. You can track the transfer of data to applications in the **Dataflow List**.
- If an application requests prior studies, remote query and remote import jobs are created, which represent querying the remote node as per the requested prior criteria, and eventually the transfer of those studies to the Modality AI solution.
- For non-interactive relevant applications, workflows are triggered automatically. You can track the workflow in the **Workflow List**.
- If an interactive application is manually triggered, the workflow is created. You can track the workflow in the **Workflow List**.
- After the workflow execution is closed and the results are created, export jobs are created for results export. Track the results export as an export job type in the **Job Queue**. Note that each results series that is ingested in the DICOM Store also appears as an ingestion job.
- If an application sends an HL7 message for priority elevation and status update, the HL7 job is created, which can be tracked in the **Job Queue**.

300018593821_A/881 * 2026-09-10

- Selecting a particular workflow in the **Workflow List** displays all the relevant jobs for that workflow in a single dialog.

To be able track a single study transfer and its related priors transfer, you can filter all the screens by **Study Instance UID**. Filters are retained across tabs.

300018593821_A/881 * 2026-09-10

www.philips.com/healthcare
healthcare@philips.com

Philips Medical Systems Nederland B.V.
Veenpluis 6
5684 PC Best
The Netherlands

© 2026 Koninklijke Philips N.V.
All rights reserved. Reproduction or transmission in whole or in part, in any form or by any means, electronic, mechanical or otherwise, is prohibited without the prior written consent of the copyright owner.

Copyrights and all other proprietary rights in any software and related documentation (“Software”) made available to you rest exclusively with Philips or its licensors. No title or ownership in the Software is conferred to you. Use of the Software is subject to the end user license conditions as are available on request.

Printed in The Netherlands

300018593821_A/881 * 2026-09-10 - en-US