

Instructions for Use

English

300018192671_A

Advanced Image Insights

Version 1.0

PHILIPS

Table of contents

1 Before You Begin 5

About the Product 5
Performance Characteristics 5
Intended Use 5
Intended Users 5
Limitations for Use 6
Errors in the Information supplied with the product 7
About the Instructions for Use 7
Accessing Instructions for Use 8
Other Instructions for Use 8
Symbols Glossary 8
Compatibility 11
Compliance 12
Safety 12
Technical Support 13
Network Safety, Security, and Privacy 13
Regulatory Controls 14
Software Updates 15
Security Issues and Guidelines 15
Implemented Security And Privacy Features 16
Additional Security and Privacy Features 16
Malware Protection 18
Microsoft Security Updates 19
De-identification 19
Data Sanitization 19
Unsecured Personal Data Transmission Risks 20
Safe Disposal of Software Components 20

2 Get Started with Advanced Image Insights 21

User Account & Login 21
Launch Advanced Visualization (AV) applications from PACS 22
Launching AV Applications from Third Party PACS 24
Using AI applications in automated flow with PACS 24
Launch Third-Party AI Applications' Accept Reject Tool from Vue PACS 25
Launch Third-Party AI Applications' Accept Reject Tool from ISPACS 25
Launch AII in Workstation Mode 26

300018192671_A/881 * 2026-07-07

Philips

300018192671_A/881 * 2026-07-07

Philips

1 Before You Begin

About the Product

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.

Intended Use

Philips' Advanced Image Insights solution provides an environment for AV/AI enablement of AV-on-cloud, third-party AI applications, and third-party applications and products, all from a single access point.

Intended Users

- Philips service engineers
- Philips cloud operation engineers

300018192671_A/881 * 2026-07-07

Philips

- Hospital IT administrators

Limitations for Use

WARNING

Operation of the product with improperly configured components could expose the patient to safety hazard(s) and could result in non-serious injury.

WARNING

Do not use Advanced Image Insights for any application until you have read, understood and know all the safety information, safety procedures and emergency procedures contained in this SAFETY section.

WARNING

Do not use Advanced Image Insights for any application until you have received adequate and proper training in its safe and effective operation. If you are unsure of your ability to operate this equipment safely and effectively DO NOT USE IT. Operation of this equipment without proper and adequate training could lead to clinical misinterpretation.

WARNING

Do not use Advanced Image Insights for any purpose other than those for which it is intended. Operation of Advanced Image Insights for unintended purposes, or with incompatible equipment, could lead to clinical misinterpretation.

WARNING

Use of this product in a way not described in these Instructions for Use, could lead to clinical misinterpretation.

NOTE

Automatic processing turnaround time (TAT) depends on network performance. Under normal conditions, it is approximately five minutes. Evaluate each application's clinical suitability with this minimum TAT in mind.

300018192671_A/881 * 2026-07-07

Philips

Errors in the Information supplied with the product

If you suspect an error in the information supplied with the software product, for example, in this Instructions for Use, you should report the error to your local Philips Representative or the Manufacturer, for analysis and, if applicable, for correction.

About the Instructions for Use

This instruction for use is intended to assist users and operators in the safe and effective operation of the product described.

- The **"user"** is considered to be the body with authority over the product.
- The "**operators**" are those persons who actually handle the product.

Before attempting to operate the device, you must read this manual thoroughly, paying particular attention to all **Warnings**, **Cautions** and **Notes** incorporated in it. You must pay special attention to all the information given and procedures described in the Safety section.



When you see this symbol, refer to the "Instructions for Use" manual that came with your system.



WARNING

Warnings are directions, which if not followed, could result in non-serious injury to a user, patient or any other person, or could lead to a misinterpretation , and/or loss or damage of patient-related data.



CAUTION

Cautions are directions, which if not followed, could cause damage to the product described in this Instructions for Use and/or any other device.

NOTICE

Notes highlight unusual points as an aid to an operator.

The "Instructions for Use" for AII are supplied electronically and/or in printed volumes. The volumes typically include:

300018192671_A/881 * 2026-07-07

Philips

- **Instructions for Use** This volume explains how to use the Philips Advanced Image Insights solution. It also contains information about safety, data security, system start-up, software navigation, accessing patient data and filming. Philips' Advanced Image Insights solution enables integration with other compatible devices and platforms. As the Instructions for Use of the integrated devices are provided separately, the Instructions for Use of Philips' Advanced Image Insights solution does not necessarily duplicate information from the Instructions for Use of other integrated devices.
- **System Administration Guide** This volume explains how to use the Philips' Advanced Image Insights solution Management application. The local site administrators and service personnel are provided the functionality required to monitor Advanced Image Insights usage, check for errors, add/delete users and groups and maintain the patient database.

Accessing Instructions for Use

The applicable Advanced Image Insights Instructions for Use documents can be easily accessed via the Philips IFU web site:
http://www.philips.com/IFU

It is also possible to search the internet for the Philips Document Library.

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 .

Other Instructions for Use

This Instructions for Use relates to Philips' Advanced Image Insights solution. However, if other software and/or equipment may be used with the software solution, each will have its own Instructions for Use.

Symbols Glossary

The following symbols may appear in the product documentation or on the labels attached to the product:

Symbol	Symbol Name	Symbol Description	Standard Number & Name	Symbol Reference Number
	Manufacturer	Indicates the name and address of the manufacturer.	EN ISO 15223-1:2021	5.1.1

300018192671_A/881 * 2026-07-07

Symbol	Symbol Name	Symbol Description	Standard Number & Name	Symbol Reference Number
	Translation Indication	Indicates that the information has undergone a translation which supplements or replaces the original information	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, section 16.3	NA
	Date of manufacture	Indicates the date when the device was manufactured.	EN ISO 15223-1:2021	5.1.3
	Batch code	Indicates the Software Release/ Version number.	EN ISO 15223-1:2021	5.1.5
	Code number	Indicates the manufacturer's catalog number so that the device can be identified.	EN ISO 15223-1:2021	5.1.6
	Consult instructions for use or consult electronic instructions for use	Indicates the need for the user to consult the instructions for use.	EN ISO 15223-1:2021	5.4.3
 **eIFU Indicator**	eIFU Indicator	Indicates an instruction to consult an electronic instructions for use (eIFU). The “consult instructions for use” symbol is accompanied by an eIFU indicator. This indicator may represent the manufacturer’s eIFU website or any other appropriate indication on the use of eIFU (e.g. “IFU Kit”).		

300018192671_A/881 * 2026-07-07

Symbol	Symbol Name	Symbol Description	Standard Number & Name	Symbol Reference Number
	Warning/Caution/ Notice Indicates that caution is necessary when operating the device or control close to where the symbol is placed, or that the current situation needs operator awareness or operator action in order to avoid undesirable consequences	**WARNINGS** are directions which if not followed could cause moderate to serious injury to an operator, patient or any other person, or could lead to a misinterpretation and/or loss or damage of patient-related data.. **CAUTIONS** are directions which if not followed could cause damage to the product described in this Instructions for Use and/or any other device. **NOTICES** highlight unusual points as an aid to an operator.	EN ISO 15223-1:2021	5.4.4
CE 0344	CE Marking of Conformity	A marking by which a manufacturer indicates that a product is in conformity with the applicable requirements set out in European Union's harmonization legislation providing for its affixing.	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices)	Annex V of MDR
Rx only	Prescription Device	Caution: In the United States, federal law restricts this device to sale by or on the order of a licensed healthcare practitioner.	21 CFR 801.109(b) (1) Prescription Devices	
MD	Medical Device Indication	An indication that the device is a medical device.	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices	

300018192671_A/881 * 2026-07-07

Symbol	Symbol Name	Symbol Description	Standard Number & Name	Symbol Reference Number
	UDI symbol	This symbol is used on the device label next to the UDI human readable indication (HRI) string.	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices	
	Importer	The symbol will be followed by the medical device importer contact details: name and address.	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, Article 13 (3)	
	Authorized Representative in Switzerland	Indicates the authorizes representative in Switzerland.	Not Applicable	

Glossary References: 1 EN ISO 15223-1:2021 Medical devices - Symbols to be used with medical devices labels, labeling, and information to be supplied - Part 1: General requirements.

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.

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

300018192671_A/881 * 2026-07-07

Philips

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.

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.

300018192671_A/881 * 2026-07-07

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:

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

Philips

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.

Technical Support

Should you encounter difficulty using Philips' Advanced Image Insights solution, contact the Philips technical support group serving your area.
For the contact information of this group, ask your local Philips representative or refer to the last page of this Instructions for Use document.

When contacting Philips technical support, have the following information available:

- Caller name, customer organization name, and location
- Site number, if applicable
- Detailed description of the problem, including any history of troubleshooting efforts completed before or after the problem first occurred

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:

300018192671_A/881 * 2026-07-07

Philips

www.philips.com/productsecurity

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.

300018192671_A/881 * 2026-07-07

Philips

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.

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.

300018192671_A/881 * 2026-07-07

Philips

User Login and Logout Protections

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

- 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.

300018192671_A/881 * 2026-07-07

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.

300018192671_A/881 * 2026-07-07

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.

300018192671_A/881 * 2026-07-07

Philips

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.

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.

300018192671_A/881 * 2026-07-07

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.

300018192671_A/881 * 2026-07-07

Philips

2 Get Started with Advanced Image Insights

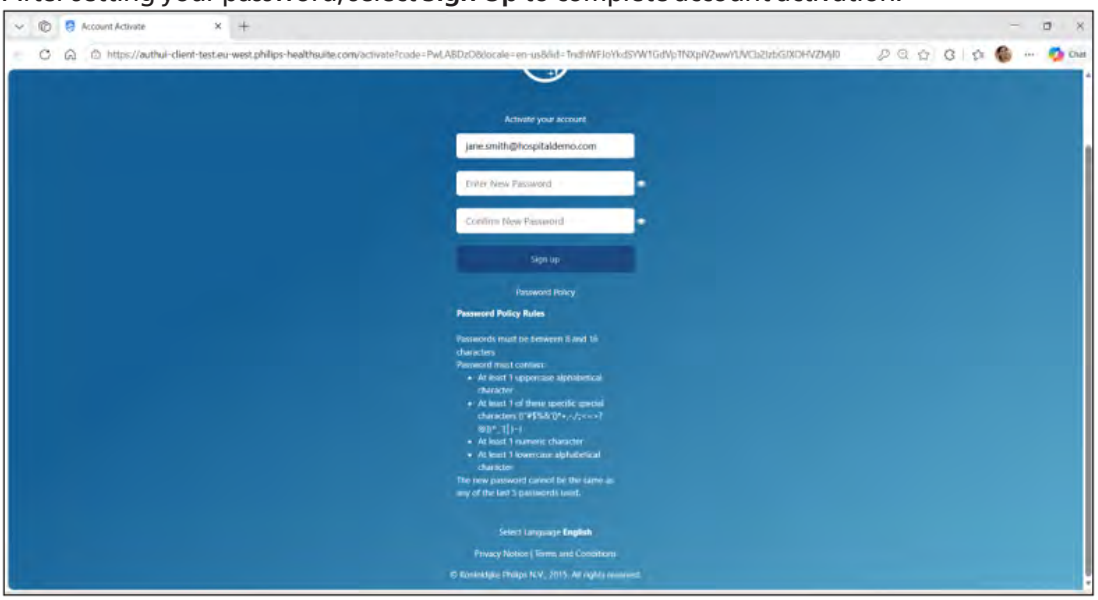
User Account & Login

Prerequisite

Access to AV applications from Advanced Image Insights (AII) is controlled via login. As a prerequisite, the user needs to be added to the Philips Identity and Access Management (IAM) system, and the account for the user needs to be activated. Follow the steps in the following section to activate the user account for the first time.

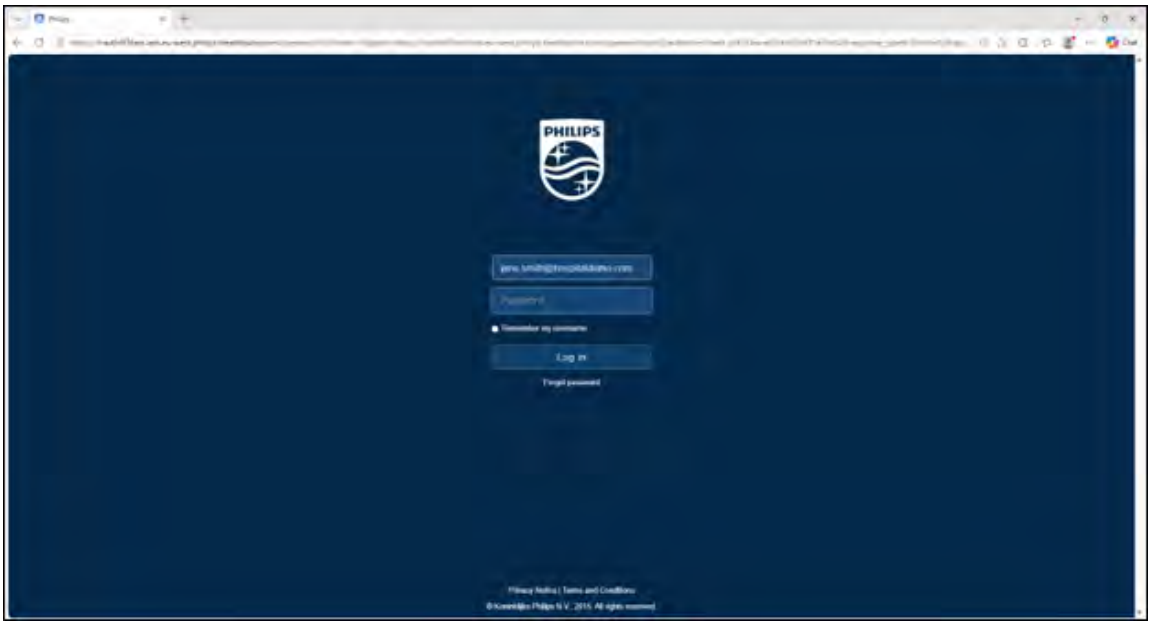
Activate a user account

1. Once a user account is created in IAM, the system automatically sends an email notification to the user.
2. Within the mail, select **Verify and activate** to activate your account and set a password. Use **Password Policy** to review the rules before creating your password
3. After setting your password, select **Sign Up** to complete account activation.



300018192671_A/881 * 2026-07-07

Login



When the Advanced Visualization Cloud application is launched from PACS or the Workstation, a login screen appears. Sign in using your username and password.

Reset a password

If a password is forgotten or expired without renewal, follow these steps to reset it:

1. On the login screen, select **Forgot Password**, enter your Login ID, and then press **Send**.
2. On the next screen, enter your email address and press **Send**. You then receive an email to reset your password.
3. From this email, select **Reset my password** to create a new password.

NOTE

After resetting, the system will not auto-redirect. You must relaunch the application to use the new password.

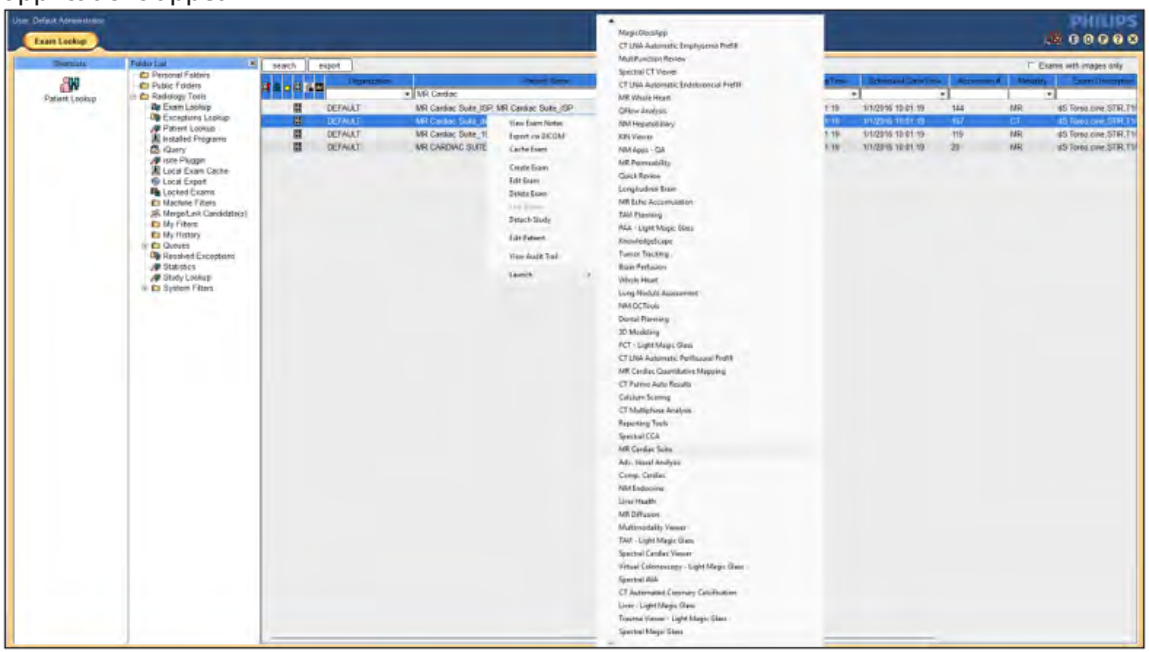
Launch Advanced Visualization (AV) applications from PACS

Launching an AV application from ISPACS

Prerequisite: Ensure the required configuration is completed in the PACS system prior to launching the application.

300018192671_A/881 * 2026-07-07

From the ISPACS worklist, select the study, right-click, and then press **Launch**. The configured applications appear.



Select an application and click to launch. Log in with your credentials.

The AV application can also be launched by opening the study, selecting the series, right-clicking, selecting **Launch**, and then selecting the application from the list. Click to launch. Once login app stream is initialized, the application launches.

Launching an AV application from Vue PACS

Select the study from the VUE Worklist, then double-click to load it.

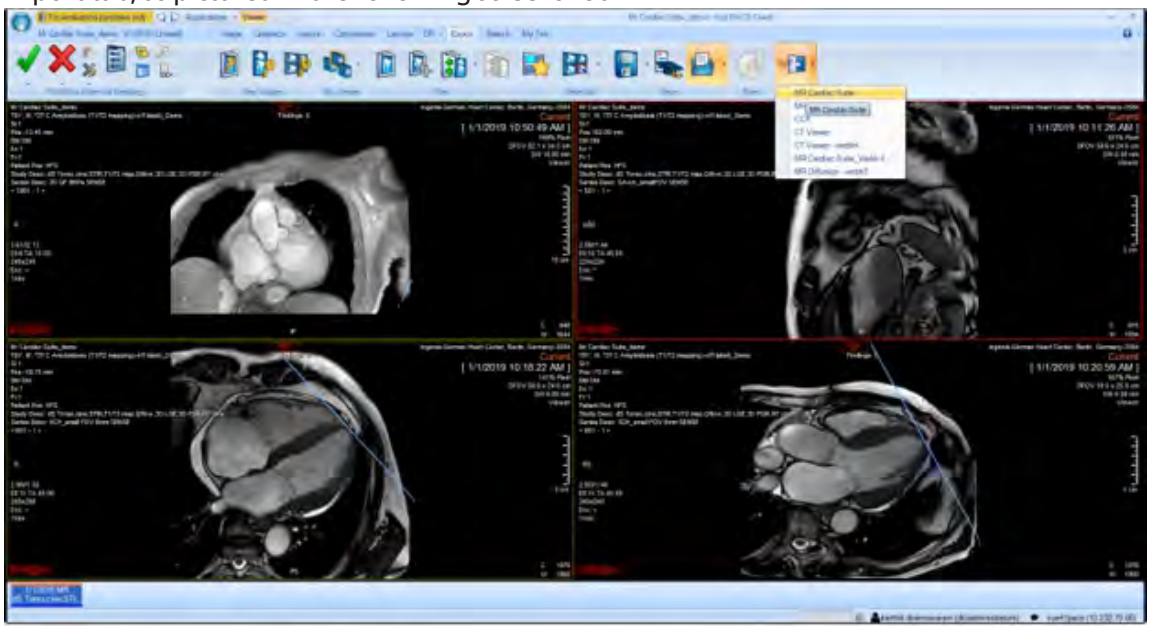
Once the study loads, go to External Applications and select the application to launch, as pictured in the following screenshot:



300018192671_A/881 * 2026-07-07

Philips

Similarly, multiple series can be selected and launched by selecting each application from the Export tab, as pictured in the following screenshot:



Launching AV Applications from Third Party PACS

Using an AV application from a third-party PACS relies on a URL-based loose integration configuration. Data exchange between PACS and AII is based on standard DICOM data exchange, with PACS sending the relevant data to DICOM Gateway.

Launching an AV application either from the toolbar, button, or right-click shortcut menu relies on PACS passing the selected data identifier, i.e study and series, in the launch request. Once the launch is done and analysis is complete, results from the AV application are transferred and available back in PACS, typically as a separate DICOM series alongside the original study.

Using AI applications in automated flow with PACS

When a new imaging study such as a CT, MRI, or X-ray is ingested into PACS, the system automatically forwards the data to the DICOM Gateway, which then routes it to the appropriate AI applications based on predefined data routing rules. The relevant AI application is triggered and begins processing the study in the background, without any manual intervention.

During this background execution, the AI application provides intermediate updates on its progress, including workflow status messages and HL7 outputs that indicate execution details and triaging status, depending on the AI application. Once processing is complete, results are returned to PACS and automatically linked to the original study, enabling radiologists to review AI findings directly alongside the original images, all without any manual intervention.

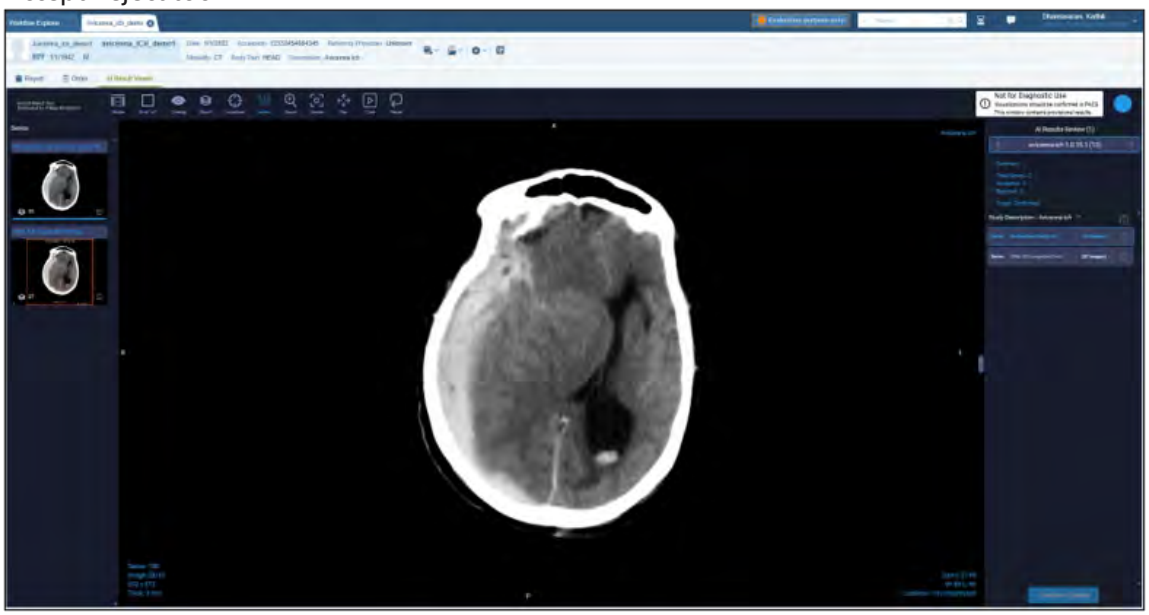
300018192671_A/881 * 2026-07-07

Philips

Launch Third-Party AI Applications' Accept Reject Tool from Vue PACS

From the Vue Worklist, choose the study and double-click to load it.

Once the study loads, select the tab **AI Result Viewer** to open the third-party AI applications' Accept Reject tool.

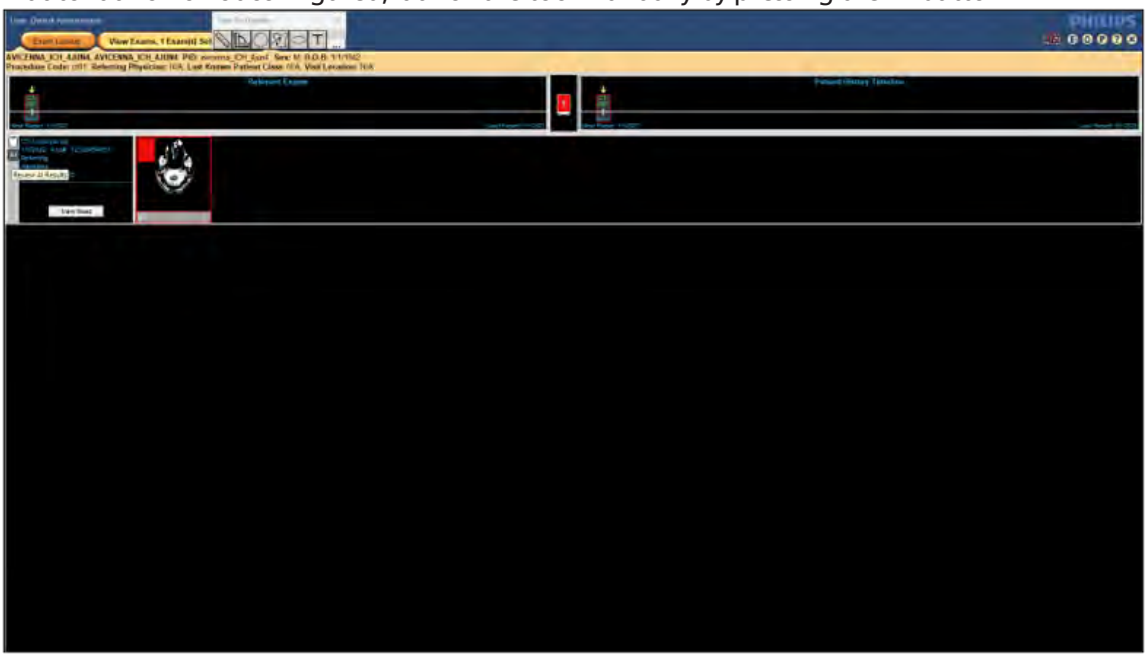


Launch Third-Party AI Applications' Accept Reject Tool from ISPACS

From the ISPACS Worklist, choose the study and double-click to load it.

300018192671_A/881 * 2026-07-07

Based on the configuration, the third-party AI applications' Accept Reject tool automatically launches with the selected study.
If auto-launch is not configured, launch the tool manually by pressing the **AI** button.



NOTE

For detailed instructions on using third-party AI applications' Accept Reject tool, refer to its Instructions for Use (IFU).

Launch AII in Workstation Mode

NOTE

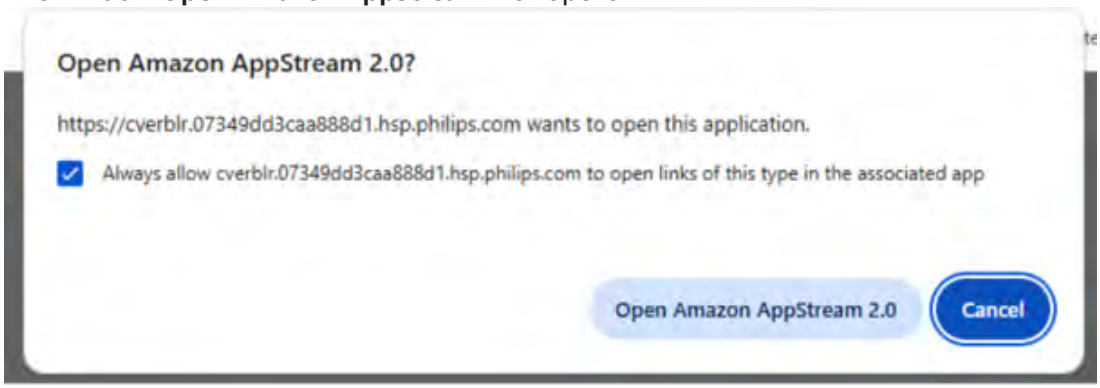
Prerequisite: Prior to using application streaming, the client software of the application streaming technology, i.e. AWS WorkSpaces Applications, must be installed and configured to use the customer-specific URL provided by Philips.

1. Open your browser and enter the application URL provided by Philips.

300018192671_A/881 * 2026-07-07

Philips

2. The window **Open Amazon AppStream 2.0?** opens.

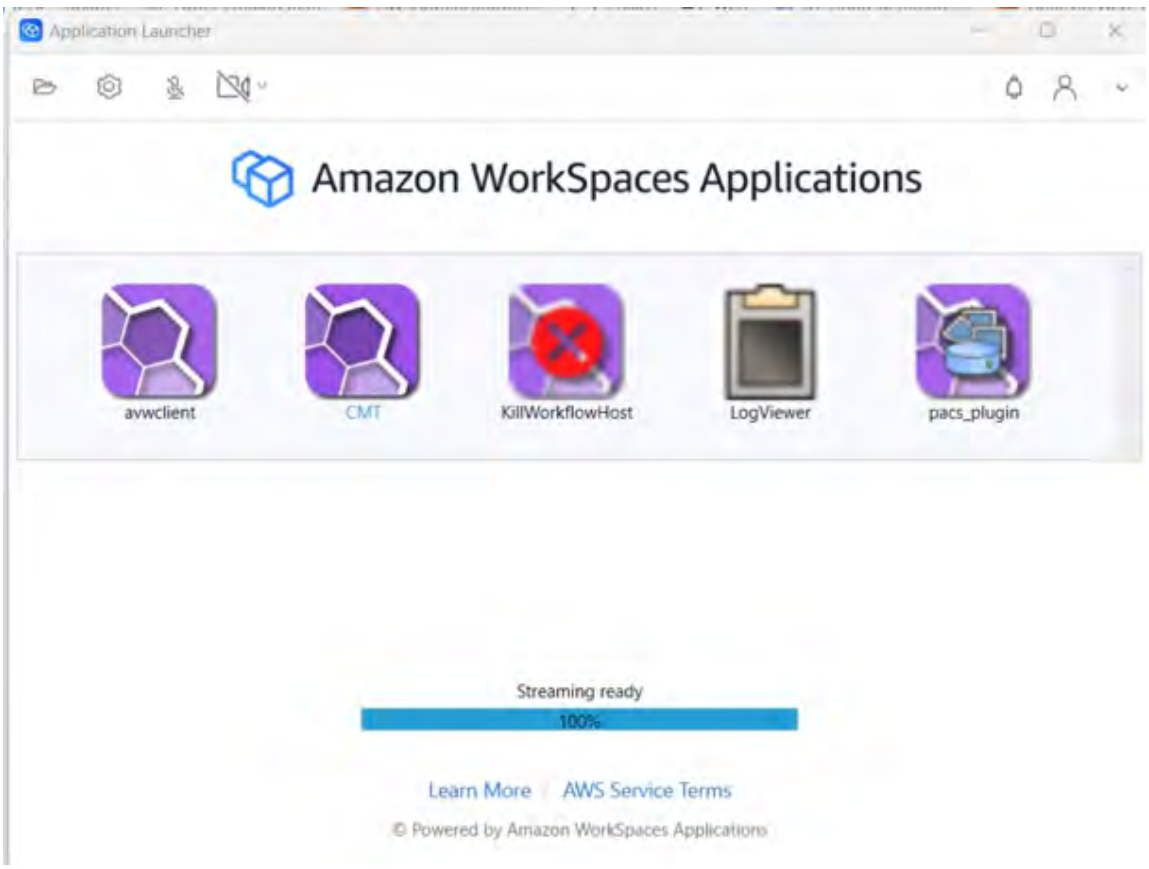


   To avoid this window in the future, select the checkbox **Always allow...**.

3. Press the button **Open Amazon AppStream 2.0**. The sign-in portal opens.
4. No login credentials are required, as credentials and permissions are used from the IA Manager login page.
5. The client launches.

Using streaming client

When launching AV using PACS Integration or Workstation mode, the Amazon WorkSpaces Applications screen appears minimized as one of the running applications in your Windows task bar.



300018192671_A/881 * 2026-07-07

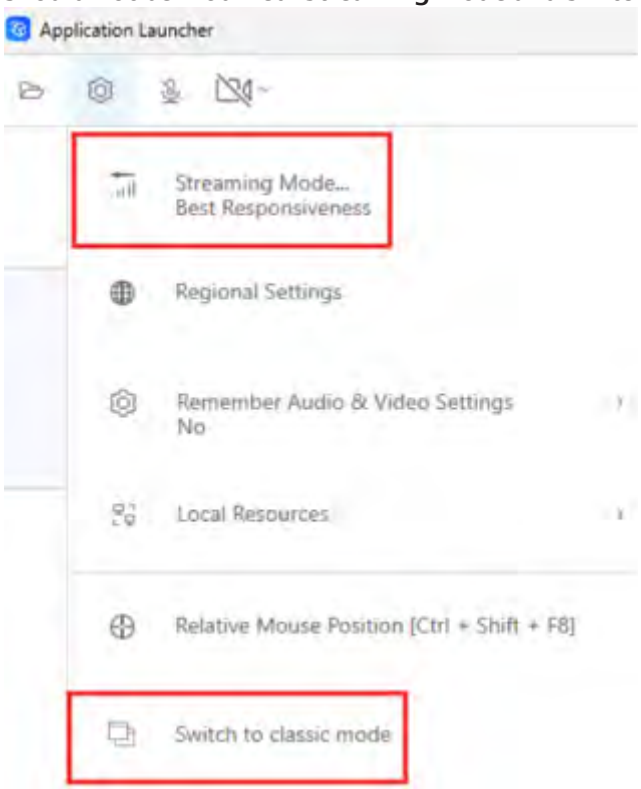
Philips

Application launcher setting

You can open application launcher settings by pressing the settings button.

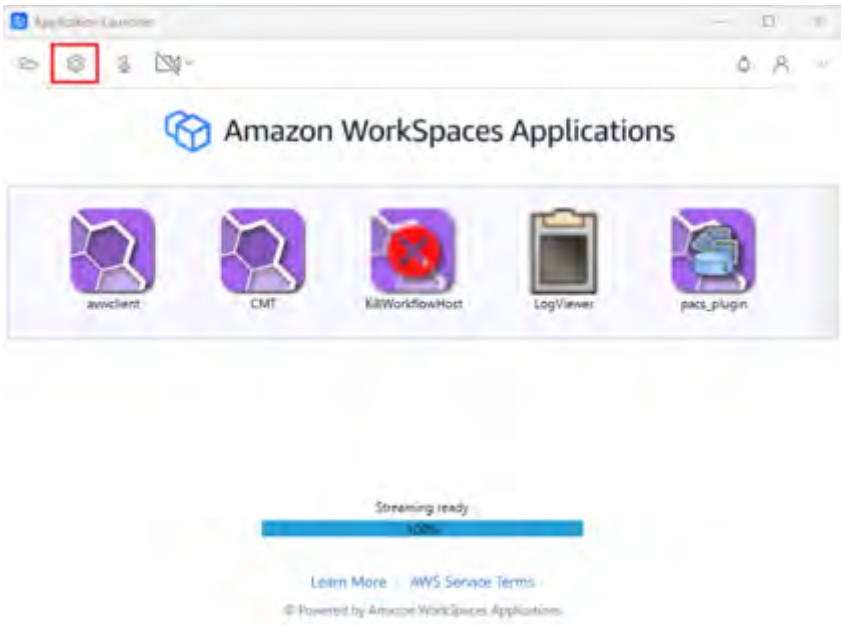
NOTE

To ensure better performance and user experience, the following streaming client settings should not be modified: Streaming mode and Switch to classic mode.



300018192671_A/881 * 2026-07-07

Allow applications inside AppStream to access files from the local computer



To enable access, open Settings, highlighted by a red box in the previous image, and then:

1. Select **Local Resources** > **Local Drives and Folders**.
2. Select which drives or folders to share from the list, or add a specific folder by using the option **Add Folder**.
3. Press the button **Save my configuration**, and then close the window.

300018192671_A/881 * 2026-07-07

Philips

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.

Microsoft is a U.S. registered trademark of Microsoft Corp.

Applicable for IT equipment that can be supplied in specific configurations:
Dell is a U.S. registered trademark of Dell Computer Corp.
HP is a U.S. registered trademark of HP Inc.

Printed in The Netherlands

300018192671_A/881 * 2026-07-07 - en-US