Vue Reporting
MModal Fluency Direct

English

D000946129 Rev D

Instructions for Use

Vue PACS

Version 12.2.8.x

PHILIPS

Table of contents

D000946129 Rev D/ * 2025-07-27

Philips

D000946129 Rev D/ * 2025-07-27

Philips

1 Before You Begin

1.1 About this guide

1.1.1 About the Instructions for Use

This Instructions for Use (IFU) 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 the 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.

WARNING

Warnings are directions, which if not followed, could cause moderate to 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.

1.1.2 Usage of product

The Instructions for Use for **Vue PACS** is supplied electronically and/or in printed volumes.

The five volumes typically include:

- *Instructions for Use*. This volume explains how to use the Vue PACS device and contains information about safety, data security, system start-up, software navigation, accessing patient data, and filming.
- *Application instructions for use volumes:*
  - Review. Depending on your version of **Vue PACS**, you may have multiple, modality-specific Review volumes (for example, CT Review; NM Review: MR Review; Multimodality Review, and so on) that explain how to use the various image viewers supplied with the system. Also included in these volumes are other processing techniques for displaying and analyzing patient studies.

D000946129 Rev D/ * 2025-07-27

Philips

  - Analysis: Depending on your **Vue PACS** version you may have multiple, modality specific Analysis volumes for example, CT Analysis; NM Analysis; MR Analysis; Multimodality Analysis, and so on) that explain how to use advanced applications.
- System Administration Guide. This volume explains how to use the **Vue PACS** device. The local site administrators and service personnel are provided the functionality required to monitor **Vue PACS** usage, check for errors, add and delete users and groups and maintain the patient database.
- Third-party applications. Different versions of Instructions for Use are available. Select the appropriate documents for your version.
- Electronic Instructions for Use. An electronic (PDF) version of the Instructions for Use is provided. Contact the administrator if you do not have access to this material.

1.2 Intended Use/Purpose

Vue PACS is an image management system whose intended use is to provide complete and scalable local and wide area PACS solutions for hospital and related institutions/sites, which will archive, distribute, retrieve, process and display medical images and data from hospital medical imaging and information systems. The system is to be used by trained professionals including, but not limited to, physicians and medical technicians

The system contains interactive tools in order to ease the process of analyzing and comparing three dimensional (3D) images. It is a single system that integrates review, dictation and reporting tools to create a productive work environment for the radiologists and physicians.

1.2.1 Intended users

The device is to be used by trained professionals including, but not limited to, physicians and medical technicians.

- Trained radiologists – to read and review medical images as part of their routine work.
- Referring physicians and clinicians – to review the images and results created by the radiologists, or access exams for review.
- PACS Administrators – to monitor and improve the efficiency, accuracy and integrity of the image services provided to the consumers.
- Patients - to view and share their images and results created by radiologists, mainly for second opinion.

1.2.2 Patient target groups and intended patient population

Vue PACS is not limited to an intended patient population nor medical condition.

D000946129 Rev D/ * 2025-07-27

Philips

1.3 Indications for use

Vue PACS is an image management system whose intended use is to provide complete, scalable local and wide area PACS solutions for hospital and related institutions/sites, which will archive, distribute, retrieve, process and display medical images and data from hospital medical imaging and information systems. This includes the display of structured reports from CAD systems with DICOM "for presentation" mammography images. The system is to be used by trained professionals including, but not limited to, physicians and medical technicians.

The system contains interactive tools in order to ease the process of analyzing and comparing three dimensional (3D) images. It is a single system that integrates review, dictation and reporting tools to create a productive work environment for the radiologists and physicians.

The system contains a Perfusion module with interactive tools to analyze and compare Computed Tomography Perfusion (CTP) and MR Perfusion (MRP) images of adult patients. Blood perfusion parameters are automatically calculated and displayed as a set of perfusion maps and perfusion tables. The perfusion tables include the calculation of parameters related to tissue flow (perfusion) and tissue blood volume.

The system contains a Diffusion Module with interactive tools to ease the process of analyzing and comparing MR Diffusion Weighted images (DWI) and MR Diffusion Tensor Imaging (DTI) of adult patients. This module is used to visualize local water diffusion properties from the analysis of diffusion-weighted MRI data.

The system supports Subtraction with interactive tools to aid with the analysis of Digital Subtraction Angiography (DSA) images in both interventional radiology and cardiology. Subtraction automatically subtracts a mask from contrast frames of an X-Ray Angiography study for visualization of vascular anatomy and pathology of adult patients.

The Lesion Management Application is a module that works with Vue PACS for measurement of lesions or regions of interest identified by trained users; tabulation of measurements, categorization of tumor response in accordance with user-selected standards, and follow-up record of findings. Lesion Management Application is not to be used for mammography.

The Vue Motion software program is used for patient management by clinicians in order to access and display patient data, medical reports, medical data, and medical images for diagnosis from different modalities including CR, DR, CT, MR, NM, ECG, and US.

Vue Motion provides wireless and portable access to medical images for remote reading or referral purposes from web browsers including usage with validated mobile devices. This device is not intended to replace full workstations and should be used only when there is no access to a workstation. For primary interpretation and review of mammography images, only use display hardware that is specifically designed for and cleared by FDA for mammography

1.4 Residual Risk

Information for safety in the form of warning, cautions, or recommendations for use has been added to the Instructions for Use, no reportable residual risks have been identified for Vue PACS.

D000946129 Rev D/ * 2025-07-27

1.5 Contraindications

There are no identified contraindications

1.6 Limitations for use

WARNING

Do not use Vue PACS 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 misdiagnosis.

WARNING

Vue PACS must be operated in an environment where the minimum specified requirements for hardware and network performance are met.

WARNING

Do not use Vue PACS for any purpose other than those for which it is intended. Operation of Vue PACS for unintended purposes, or with incompatible equipment, could lead to clinical misdiagnosis.

WARNING

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

WARNING

The Vue PACS system can display both lossless and lossy compressed images. The user's ability to analyze images depends on the quality of the image data the user intends to analyze. Lossy/Irreversible compression affects the quality of the image. The user is responsible to ensure that the image's quality is adequate enough for the review purpose.

WARNING

When running Vue PACS with a virtualization solution (Citrix XenDesktop®), a degradation in image quality, in addition to skipped frames, can occur, based on the network bandwidth and virtual machine configuration.

D000946129 Rev D/ * 2025-07-27

Philips

WARNING

Before the study is closed, verify that images are copied or backed up successfully.

WARNING

Before the study is deleted, verify that images are copied, archived or backed up successfully.

WARNING

Be careful when editing the report. In some parts of the report it is possible to change the information created automatically.

WARNING

Make sure that you are using appropriate monitors and that they are properly configured and calibrated prior to using Vue PACS especially for clinical application such as Mammography.

WARNING

Never switch the IT equipment off using the POWER ON/OFF switch while the software product is still running, as this can damage data integrity, which can lead to loss or damage of patient-related data. Always exit the software product before switching off the IT equipment.

WARNING

Do not install unsupported software on the Vue PACS system because this could interfere with diagnosis or interpretation, or cause loss of or damage to patient-related data, and/or introduce computer viruses.

CAUTION

In case of a failure and images are not available via PACS, if the images need to be viewed immediately, physician/radiologist shall refer to the modality itself. When there is no onsite radiologist that can access the modality, the Institute guiding principles and procedures shall be followed.

D000946129 Rev D/ * 2025-07-27

Philips

1.7 Symbols Glossary - Non-Medical

Symbol	Symbol Name	Symbol Description	Standard / Regulation Number & Name	Symbol Reference Number
	Manufacturer	Indicates the name and address of the manufacturer.	EN ISO 15223-1:2021 [1]	5.1.1
	Date of manufacture	Indicates the date when the device was manufactured.	EN ISO 15223-1:2021 [1]	5.1.3
	Batch code	Indicates the Software Release/ Version number.	EN ISO 15223-1:2021 [1]	5.1.5
	Code number	Indicates the manufacturer's catalog number so that the device can be identified.	EN ISO 15223-1:2021 [1]	5.1.6

D000946129 Rev D/ * 2025-07-27

Symbol	Symbol Name	Symbol Description	Standard / Regulation Number & Name	Symbol Reference Number
	Consult instructions for use	Indicates the need for the user to consult the instructions for use.	EN ISO 15223-1:2021 [1]	5.4.3
 **eIFU Indicator**	eIFU Indicator	When used to indicate an instruction to consult an electronic instructions for use (eIFU), this symbol is accompanied by an eIFU indicator. This indicator can represent the manufacturer's eIFU website or any other appropriate indication on the use of eIFU (for example, "Refer to IFU Kit"). The indicator can be placed either alongside, beneath, or surrounding the symbol.		

D000946129 Rev D/ * 2025-07-27

Symbol	Symbol Name	Symbol Description	Standard / Regulation Number & Name	Symbol Reference Number
 or  or 	Warning/Caution/ Notice This symbol is used on the device label to highlight the fact that there are specific warnings or precautions associated with the device, which are not otherwise found on the label.	**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 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 or any other device. **NOTICES** Notes highlight unusual points as an aid to the operator.	EN ISO 15223-1:2021 [1]	5.4.4
	Unique Device Identifier	Indicates a carrier that contains the unique device identifier information. This symbol must be placed adjacent to the Unique Device Identifier Information.	EN ISO 15223-1:2021 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, Annex I.	5.7.10
	Importer	Indicates the entity importing the medical device into the locale. The symbol will be followed by the medical device importer contact details: name and address.	EN ISO 15223-1:2021 Article 13 (3) MDR	5.1.8

D000946129 Rev D/ * 2025-07-27

1.8 Compatibility

The software product described in this Instructions for Use must not be used in combination with other software, equipment or components unless such 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.

Changes and/or additions to the server or workstation must only be carried out by Philips or by third parties expressly authorized by Philips to do so. Such changes and/or additions must comply with all applicable laws and regulations which have the force of law within the jurisdictions concerned, and with best engineering practice.

Changes or additions to the software product that are carried out by persons without the appropriate training or using unapproved spare parts can lead to the Philips warranty being voided.

Philips is not responsible for any malfunction of Vue PACS, if Vue PACS runs on hardware that is not according to hardware specification.

If not supplied by Philips with the Vue PACS software, Philips is not responsible for any malfunction of the hardware used.

1.9 Compliance

Vue PACS complies with relevant international and national standards and laws.

Information on compliance will be supplied on request by your local Philips Representative or by the Manufacturer.

This software product must 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.

1.10 Training

Users of the Vue PACS device must have received adequate training on its safe and effective use before attempting to use the software product described in this Instructions for Use.

Training requirements for this type of software product will vary from country to country. It is for users to make sure that they receive adequate training in accordance with local laws or regulations, which have the force of law. If you require further information about training in the use of this software product, contact your local Philips representative or the Manufacturer.

D000946129 Rev D/ * 2025-07-27

Philips

1.11 Technical support

Should you encounter difficulty using **Vue PACS**, contact the Philips technical support group serving your area. To obtain contact information for this group, ask your local Philips representative.

When contacting Philips technical support, please 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.

For contact details, browse to www.philips.com/healthcare

1.12 Safety

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

Also see the following information:

- Intended use of Vue PACS. See Intended Use/Purpose in this IFU.
- Contraindications. See Contraindications in this IFU.
- Training for operators of Vue PACS. See Training in this IFU.

NOTICE

Any serious incident that has occurred in relation to the device should be reported to the manufacturer or its EU Authorized Representative and also reported to the local competent authority of the European Union / European Free Trade Association member state in which the user or patient is established. Reporting in other jurisdictions must follow the applicable local regulations.

D000946129 Rev D/ * 2025-07-27

Philips

1.13 Network Safety, Security and Privacy_default

1.13.1 General

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, multilayered strategy (including policies, processes, and technologies) to protect information and systems from external and internal threats.

Adhering to industry-standard practice, adopt the following strategy:

- Physical security
- Operational security
- Procedural security
- Risk management
- Security policies
- Contingency planning

The actual implementation of technical security elements varies by site and might employ several technologies, including firewalls, VLANs, NIDS, virus-scanning software, authentication methods, and other technologies.

As with any computer-based system, protection must be provided so that firewalls and 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 must 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.

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 at:

http://www.philips.com/productsecurity

NOTICE

Philips is not responsible for security of hospital-managed systems (desktop PCs, laptops) where the Vue PACS viewer is installed.

1.13.2 Protecting Patient Health Information

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

D000946129 Rev D/ * 2025-07-27

Philips

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

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

1.13.3 Preventing Unauthorized Device Modification

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

Operators of this medical device must permit only Philips-authorized changes to be made to the servers (or viewers, if applicable), either by Philips' personnel or under Philips' explicit published direction.

1.13.4 Software Installation

CAUTION

Installation of software not authorized by Philips or not specified in the Vue PACS system documentation can adversely affect the operation and security of the system, in addition to the networks to which the system is connected. These adverse effects might not be immediately apparent to the user. Therefore, users must not install unauthorized software onto the Vue PACS Server and Workstation.

1.13.5 Off-the-shelf Software

The Vue PACS system can be used with the following customer-supplied off-the-shelf software products on local computer workstations and file servers.

Manufacturer	Name	Version
Microsoft	Windows Server	2019
Microsoft	Windows Desktop	10/11

1.13.6 About Screen

To display the About screen that displays labeling and product information, open the application, select **Help** then from the menu select **About**.

1.13.7 Software updates

Updates for this Philips software product can become available. Such updates will be communicated by Philips. Some of these updates are specific security patches and some are maintenance releases and are essential to keep the software product operating securely, safely, effectively, and reliably.

D000946129 Rev D/ * 2025-07-27

1.13.8 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 must be understood and addressed by operators and owners. This applies to the Vue PACS Server and Workstation and not to the diagnostic viewer PCs.

Network security

The Vue PACS system 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, NIDS (Network Intrusion Detection System), the use of VLANs, and virus scanners.

CAUTION

The Vue PACS system does not require open Internet connectivity for its standard Intended Use. It is strongly recommended that the Vue PACS Server/Workstation not be used for Internet browsing.

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:

- Automatic generation of alerts for Vue PACS server critical issues
- Assistance for workstations
- Remote assistance for servers
- Distribution of software
- Installation of software

Positioning of display monitors

Unauthorized visual access to protected information can be minimized by positioning the system's display monitor so it faces a wall, to prevent viewing from doorways, hallways, and other traffic areas.

D000946129 Rev D/ * 2025-07-27

Philips

NOTICE

- Monitor position is a suggestion for use with monitors of the Vue PACS viewer PCs and the Vue PACS Workstation.
- To help in limiting unauthorized visual access, an unattended computer display automatically goes blank after a set period of time.
- The Vue PACS system supports Automatic Logoff/Screen Lock. For additional information, see Automatic logoff (Lock Screen).

Room and equipment access controls

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

Access to the room containing the Vue PACS server or workstation must be controlled by policy and procedures that identify who is authorized to occupy specific areas.

The following physical controls are a recommended baseline and not a comprehensive list. 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:

- Physically accessible computers containing personal data should be kept under lock and key.
- Require the use of physical tools or keys to access components that store data within the system.
- Employ anti-tampering mechanisms and be capable of detecting unauthorized physical access to Internal devices that store personal data, such as hard drives.
- Deploy anchors or locks to physically secure portable components or sub-components that store personal data.
- Disable or lock unnecessary I/O device interfaces and devices on physical servers and workstations (for example, network, CD, DVD USB, serial sockets, and so on).

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 system and user account passwords periodically.

D000946129 Rev D/ * 2025-07-27

Philips

CAUTION

It is strongly recommended that the password of pre-defined user accounts (OS and application) on the Vue PACS system, be changed at the time of system deployment in your facility. Consider changing these passwords on a periodic basis in accordance with your healthcare facility policy and industry standard best practices. Contact your Philips Service Engineer for more details.

Removable and portable media

When using removable media like USB storage devices, CDs, and DVDs, be aware of these security and privacy issues:

- Inserting removable media can introduce a virus to the medical device.
- If removable media is used to store patient data, protect the information from media obsolescence and potential data loss by planning and performing data migrations to newer storage technologies.
- If the removable media is to be stored for safekeeping, protect the data from “fading” loss by performing media renewal as recommended by the media manufacturer and storing it in a secure location according to manufacturer recommended environmental settings.

CAUTION

Whenever media is inserted into the Vue PACS system, make sure that the media has not been exposed to viruses, worms, and Trojans. Make sure the media has been scanned for viruses or malware before connecting it to server or workstation and each use.

CAUTION

It is not possible to prevent the transfer of data to removable media.
Removable media used in conjunction with the Portal Server for data transfer purposes, can contain confidential patient information. Take appropriate measures to protect this information, so that unwanted access by unauthorized individuals is avoided.

CAUTION

Removable media that contains images and other medical information must be stored in a secure area that is not accessible by unauthorized individuals.

D000946129 Rev D/ * 2025-07-27

CAUTION

If the removable media containing patient data, images, or sensitive information is to be discarded, it must be destroyed (or the contained data permanently deleted) so that the data stored on it can no longer be accessed. Data that is deleted from removable media using conventional operating system or application tools will still be present on the media and data sanitization must be performed. While the Vue PACS system has data deletion capabilities, it does not provide data sanitization functionality for media that contain patient data or other sensitive information. Use appropriate data sanitization techniques and tools along with healthcare entity policies regarding media destruction and sanitization. NIST publication 800-88 Guidelines for Media Sanitization provides guidelines and best practices for media sanitization.

1.13.9 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 Vue PACS system.

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 assigned to application-based roles. Philips strongly advises to adhere to the least privilege principle.
- Access to the system is enabled through Username/password authentication, or other mechanisms like two factor authentication, smart cards, URL activation and OpenID Connect.
- Password complexity rules can be defined through the User Management tool.
- Password expiration rules can be defined through the User Management tool.
- Account Lockout Policy can be defined through the User Management tool.

  The application account Lockout Policy is:

  – Account lockout duration = 1 minute

  – Bad login attempts = 10
- This can be customized through the User Management tool
- • Philips strongly advises to remove a user from the system as soon as possible in case of termination of the contract.

D000946129 Rev D/ * 2025-07-27

Automatic logoff (Lock Screen)

The Vue PACS system provides a configurable idle time-out feature. The time-out configuration can be done using the Vue PACS tool. Only a system administrator can disable the automatic logoff feature.

After an inactivity time-out, the Lock screen appears (with the last logged in user displayed).

Additionally, automatic logoff can be accomplished through Microsoft Active Directory group policies.

Audit trail

It is required to log user activities that are information-security critical:

- This applies to logging-on, reading, or modifying clinical information.
- The system supports detailed audit trail logs, which are IHE ATNA compliant.
- The audit trail logs are either stored locally in an encrypted form on the system or can be transferred to a central Syslog server.
- Local audit logs can be viewed using the Audit Log Viewer. The Audit Log Viewer can be accessed by hospital administrators from the IT Tools folder present on the desktop of the Vue PACS system.

1.13.10 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 later. This section also lists other information related to security features that are not implemented and of which the owner of the systems must be aware.

1.13.11 Backup procedure

The system is permanently storing sensitive patient personal information, which is stored on the Oracle database and on the local storage. Personal information is encrypted.

1.13.12 Disaster recovery and business continuance

Vue PACS is a platform used in the diagnosis and treatment planning of patient care. In the event of a major outage or disaster, make sure that Vue PACS is a part of the healthcare entities Business Continuance (BC) and Disaster Recovery (DR) plan. Consider addressing the following key points for the BC and DR plan:

- Make sure that the healthcare entity has a reliable and consistent Business Continuance (BC) and Disaster Recovery (DR) plan. The Vue PACS system must be a part of DR/BC plan to ensure that it is readily recoverable and usable in the event of an unplanned outage or major disaster.

D000946129 Rev D/ * 2025-07-27

- Make sure that copies or replication is occurring for all required Vue PACS data. It is recommended to maintain the data in a separate datacenter and geographical area according to the healthcare entities DR/BC plan.
- Update the BC/DR plan as necessary to ensure that it is accurate and usable. The healthcare entity BC/DR plan must reflect any changes made to the production Vue PACS system.
- Ensure that the BC/DR plan is periodically tested and according to the healthcare entities policies and procedures. Confirm that the Vue PACS system will be recoverable within the expected Recovery Time Objective (RTO) of the healthcare entity.

1.13.13 Emergency access procedure

The Vue PACS 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. Hospital administrators can use this function to create an emergency user account and complex password with the necessary permissions. To avoid unauthorized access to patient data, make sure that knowledge of this generic emergency user account and password is restricted and kept in a secure location with minimal access.

The Vue PACS system does not allow or enforce generic account users to enter their real names, which restricts the system's ability to track and audit the generic user account.

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

1.13.14 Encryption

Vue PACS supports encryption through several different methods to ensure that information is protected and secure.

Encryption at rest is supported by using SEDs (Self Encrypting Drives), which must be supplied by the healthcare facility or purchased through Philips. The use of software-based encryption at rest such as Microsoft BitLocker is not supported at this time.

Vue PACS uses three primary encryption protocols for data in transit between the endpoints and the servers. The site will need to supply SSL/TLS certificates for those services that require encrypted communications.

The following primary services or protocols offer encryption as part of their communication processes.

- CONN (proprietary protocol) for internal services
- DICOM for to communicate with devices that supports the DICOM standard
  - Vue PACS system supports the IHE ATNA profile, which enables secure transmission of ePHI between configured DICOM devices.
- HTTPS for web services

Vue PACS supports TLS 1.2 protocol for encrypted communication processes.

D000946129 Rev D/ * 2025-07-27

Philips

1.13.15 Physical access to system

The Vue PACS system must be placed in an access restricted area of the hospital.

However, the following characteristics are to be taken into account for system operation and access control when the hardware is purchased from Philips:

- The computer case is "service friendly" (for example, accessing and removing the hard drive does not require tools). However, the computer case can be locked (for example, by cable lock).
- The boot order for the system is DVD, USB, hard disk. By inserting bootable CD/DVD or connecting bootable USB memory device, the system can start up from those and thus access can be gained to the system including information stored in it.
- There is no detection of unauthorized physical access into the system (for example, through tamper-proof seals).
- Unauthorized changes to software, files or data on the Vue PACS system are not permitted and by doing so might 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.

1.13.16 Malware protection

The Vue PACS system incorporates protection mechanisms against the intrusion of malware (viruses and so on). Without proper cybersecurity maintenance, 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 remains that the equipment might become infected with malware. When malware is detected, or when you notice that unfamiliar behavior or degraded performance occurs repeatedly, immediately call the Philips Service Engineer for an inspection.

When the inspection confirms the infection, be sure to take measures to contain and remove the source of infection. As necessary, Philips Service can reinstall the product`s software to bring the product back into specification.

1.13.17 Whitelisting

Philips formally qualifies the Vue PACS system with CylancePROTECT®/Trend Micro, aimed at providing comprehensive malware protection using whitelisting technology.

Whitelisting identifies all trusted software that is allowed to execute on the equipment. The protection software thus prohibits the execution of untrusted software, effectively blocking malware before damage is done. Instead of relying on the frequent updates that the reactive anti-virus software needs to remain up-to-date, it offers proactive protection against a wide spectrum of malware and malware alterations by only allowing known executables. Whitelisting is not a replacement for industry standard anti-virus solutions, but it is a complementary foundation for enhanced protection against malware intrusion and unwanted code execution.

D000946129 Rev D/ * 2025-07-27

Philips

Philips certified anti-virus software

Philips formally qualifies the Vue PACS system with CylancePROTECT®/Trend Micro, aimed at providing comprehensive malware protection using whitelisting technology. Whitelisting identifies all trusted software that is allowed to execute on the equipment. The protection software thus prohibits the execution of untrusted software, effectively blocking malware before damage is done. Instead of relying on the frequent updates that the reactive anti-virus software needs to remain up-to-date, it offers proactive protection against a wide spectrum of malware and malware alterations by only allowing known executables.

The installation of anti-virus software will not automatically void the equipment warranty or service contract. Philips can provide limited support and resolve most incidents reported by the customer in a timely manner and typically within the Service Level Agreement. However, due to the dynamic nature of anti-virus software and ongoing updates, Philips cannot be held accountable for any downtime or deletion of data caused or allowed by the anti-virus applications due to subsequent updates. Any efforts to resolve issues or problems arising from the installation or actions resulting from the anti-virus software are not covered by the Service Agreement or warranty and may result in time and materials charges. In addition, Philips may request that the anti-virus software be removed or disabled to proceed with the resolution of reported issues or for system upgrade. Philips may also request that the customer provide evidence of the specific malfunction on the system without anti-virus software installed and/or enabled.

NOTICE

The anti-virus software that is validated and approved might change over time. If you have a question related to alternate anti-virus software, contact your respective Philips Service Engineer.

CAUTION

Installing alternate anti-virus software on the Vue PACS server is an action taken by the hospital IT administrator.
The sole responsibility of such an action and its impact rests with the healthcare entity IT.

1.13.18 Endpoint Protection

CylancePROTECT comes standard on Philips for Vue PACS 12.0 and is an endpoint security product that detects and prevents various cybersecurity threats. Below is a description of cybersecurity events that CylancePROTECT can detect and how users are informed of such events:

Malware Detection:

- Event Description: CylancePROTECT can detect and block malware, including known and unknown threats, by analyzing file behavior and characteristics.

D000946129 Rev D/ * 2025-07-27

Philips

- User Notification: Users are typically informed through a real-time pop-up notification on their endpoint devices, indicating the detection and containment of the malware. The notification may provide guidance on next steps, such as isolating the affected device or initiating a malware scan.

Suspicious File Execution:

- Event Description: CylancePROTECT can flag suspicious or unauthorized file executions, such as the launching of unknown or potentially harmful applications.
- User Notification: Users will receive immediate notifications on their devices, alerting them to the suspicious activity. They may be advised to avoid interacting with the file or application and contact their IT support team for further assistance.

Script and Macro Detection:

- Event Description: The product can identify malicious scripts and macros often used in attacks like phishing or document-based threats.
- User Notification: Users may receive alerts when opening documents or running scripts containing suspicious elements. They will be instructed to exercise caution and contact IT support for guidance.

Exploitation Attempts:

- Event Description: CylancePROTECT can detect and prevent exploitation attempts targeting known vulnerabilities in software or operating systems.
- User Notification: Users may receive alerts if an exploitation attempt is detected while interacting with a vulnerable application or system. They will be advised to apply necessary updates or patches to mitigate the risk.

Device Quarantine:

- Event Description: If a device is compromised or poses a significant threat, CylancePROTECT can automatically quarantine or isolate the affected device from the network.
- User Notification: Users will be notified of the quarantine action, typically through a notification on their device, informing them of the security measure taken. IT administrators will also be alerted to assess and remediate the issue.

Threat Intelligence Updates:

- Event Description: CylancePROTECT regularly receives threat intelligence updates to stay updated on the latest cybersecurity threats and attack patterns.
- User Notification: Users are typically not directly informed of threat intelligence updates. Instead, the product silently updates its threat database in the background to enhance its threat detection capabilities.

Policy Violations:

- Event Description: CylancePROTECT can enforce security policies and detect policy violations, such as unauthorized software installations or access to restricted resources.
- User Notification: Users will receive notifications if they attempt to violate security policies. The notification will provide guidance on complying with company policies and security best practices.

D000946129 Rev D/ * 2025-07-27

Philips

1.13.19 Microsoft security updates

Microsoft Security Updates are routinely included with each new software release. Alternatively, Philips permits the installation of Microsoft® security updates on the Vue PACS system.

For a list of approved or validated Microsoft® security updates for Vue PACS Server/ Vue PACS Workstation, see the vulnerability evaluation report, known as the Security Status document.

The documents are accessible using the following link: www.philips.com/security.

Philips strongly advises not to apply any OS or other patches until Philips has validated it for use with the 12.0 product.

After the web page loads, click the option/image for "Cyber-security information of Philips healthcare products". A new web page will open. Follow the guidelines provided to first request access to the product security documentation and subsequently to access the document distribution platform, Philips InCenter. In Philips InCenter, look for the product group "Radiology Informatics (RI)" to find the Security Status documents for the Vue PACS product with reference to the Security Status document. Philips permits customers to install only security updates that 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. Customers can download the respective Microsoft security update referenced by the unique Microsoft® KB number from the Microsoft® TechNet website or access the same from an internal server/repository. Ensure that you download and access only the updates that are applicable to the Microsoft® Operating System used on the Vue PACS system, that is, only updates intended for one of the following (depending on the Vue PACS product variant that you have purchased):

- Windows Server 2019 (x64) OS.

1.13.20 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 Vue PACS Instructions for Use, under the Saving Images/Copying to Studies with Concealed Patient Information section.

1.13.21 Data sanitization

Vue PACS stores patient sensitive data within the system Oracle database and DICOM images. Media containing backups of the database and images will contain patient or sensitive data as well.

Patient or sensitive data can be stored in the following locations of the Vue PACS system:

- Oracle database folder
- System Oracle database backup storage folder
- Customer defined image storage locations (local or network)

D000946129 Rev D/ * 2025-07-27

Philips

If patient data, images, or sensitive information resident on the Vue PACS 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 that is deleted from storage using conventional operating system or application tools will remain but not directly usable on the storage media. Data sanitization must be performed for permanent deletion. While the Vue PACS system 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.

1.13.22 Unsecured personal data transmission risks

Vue PACS 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) for all Web and DICOM services to ensure the secure transmission of data to the client device or modality. Please note that the healthcare entity might need to purchase or provide valid TLS certificates.

D000946129 Rev D/ * 2025-07-27

Philips

1.13.23 Safe disposal of software components

Before disposing of the Vue PACS software components, Vue PACS server and workstation drivers must be formatted in order to ensure that patient data is securely removed and cannot be recovered.

D000946129 Rev D/ * 2025-07-27

2 Introduction

Vue Reporting can use the M*Modal Fluency Direct speech recognition engine for dictating reports.

The M*Modal Fluency Direct is installed locally on the Desktop Diagnostic Viewer workstation and is synchronized against the M*Modal Cloud that provides the voice recognition services for the users.

This document is intended for the end users (radiologists).

NOTICE

This document lists only the M*Modal Fluency Direct features that are relevant when it is used as the main speech recognition engine.

For further details about using Vue Reporting, see the **Vue Reporting User Guide**.

2.1 Before You Begin

This document may describe features that are optional and require a special license to run.

If they are not available on your system, contact Philips for further details regarding license and feature upgrades.

D000946129 Rev D/ * 2025-07-27

Philips

D000946129 Rev D/ * 2025-07-27

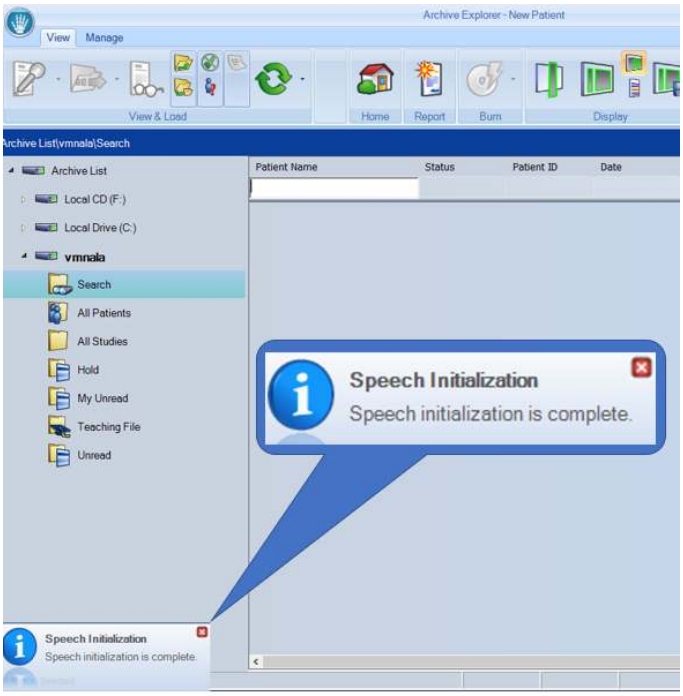
Philips

3 Calibrate Your Microphone

To calibrate your microphone, perform the following steps:

1. Connect your microphone device to the Desktop Diagnostic Viewer workstation.
2. Enter your username and password to log in to the Desktop Diagnostic Viewer.

3. On your first login to the Desktop Diagnostic Viewer, the Speech Initialization process is performed and completes successfully.



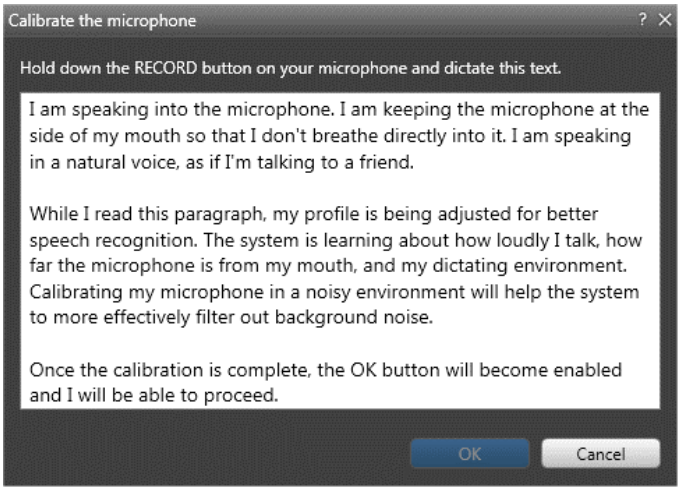
4. When the **Calibrate the microphone** window appears, start recording then read the text to complete microphone calibration.

NOTICE

In this client version, use the 'Play' button on the SpeechMike to start the recording in the 'Calibrate the microphone' window.

This will work in an On/Off mode (i.e. not in a dead-man switch mode)

You can also manually load the Calibrate the microphone window from the Report Editor by clicking the Audio Wizard button from the Recognition tab.



D000946129 Rev D/ * 2025-07-27

4 Manage Your Dictionary

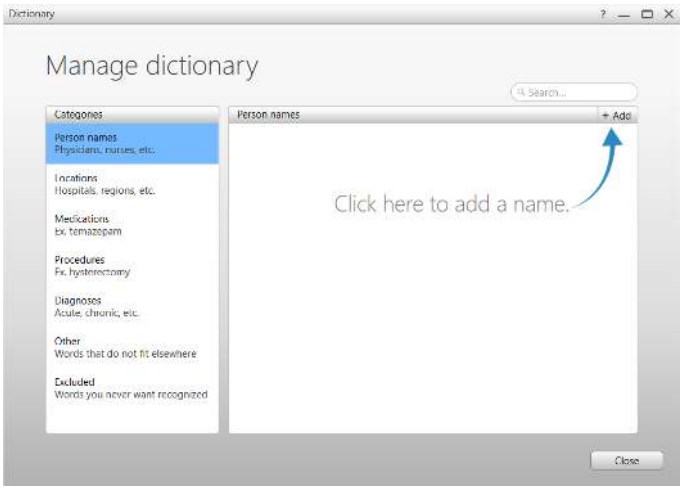
Use the dictionary to:

- Add new words to your dictionary that do not exist.
- Improve recognition of existing words by familiarizing the system with your acoustic qualities.

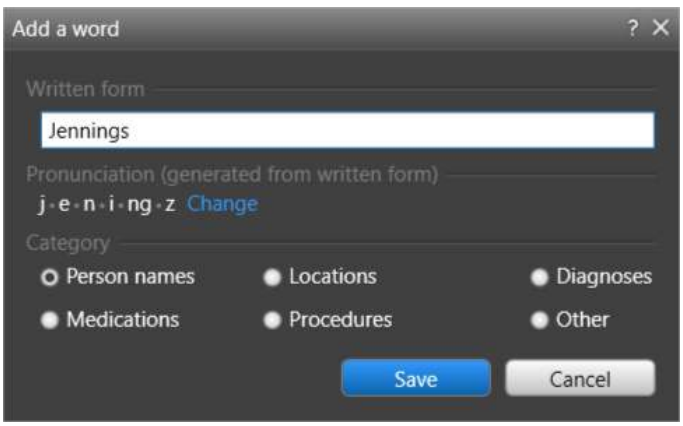
The Personal Lexicon Manager (PLM) allows you to add, train, or delete words from your personal dictionary.

To add new words, perform the following steps:

1. From the **Report Editor**, click the **Personal Lexicon Manager**  button under the **Recognition** tab.
2. From the left pane, select the most appropriate category where you would like to add the new word then click **Add**.



3. In the **Add a word** dialog, type in the word that you want to add then click **Save**.

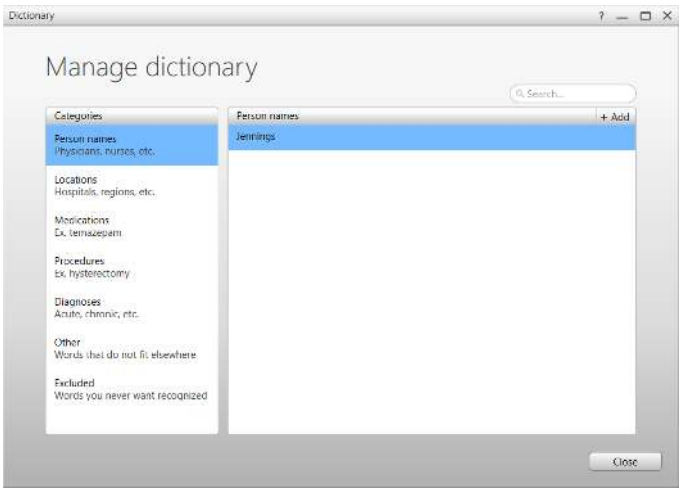


4.1 Training the System to Enhance Recognition

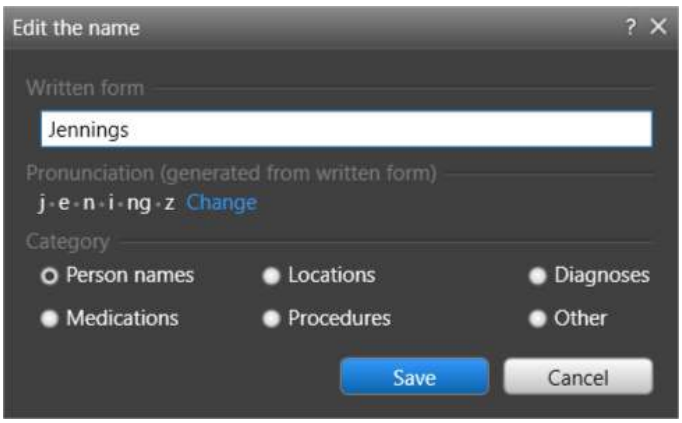
For certain words you may find that you need to better familiarize the system with your specific vocal qualities to prevent cases where words that exist in the lexicon fail to be recognized by the Editor and therefore do not appear correctly when you use them in your dictation.

To train the system to enhance recognition, perform the following steps:

1. From the **Dictionary** window, click the word that you want to train.



2. In the **Edit the name** dialog, click **Change**.



3. Select **Record pronunciation**.

D000946129 Rev D/ * 2025-07-27

4. To train the system, start recording, dictate the word and then stop recording.
5. Verify that your record pronunciation looks correct, click the **OK** button then click **Save**.

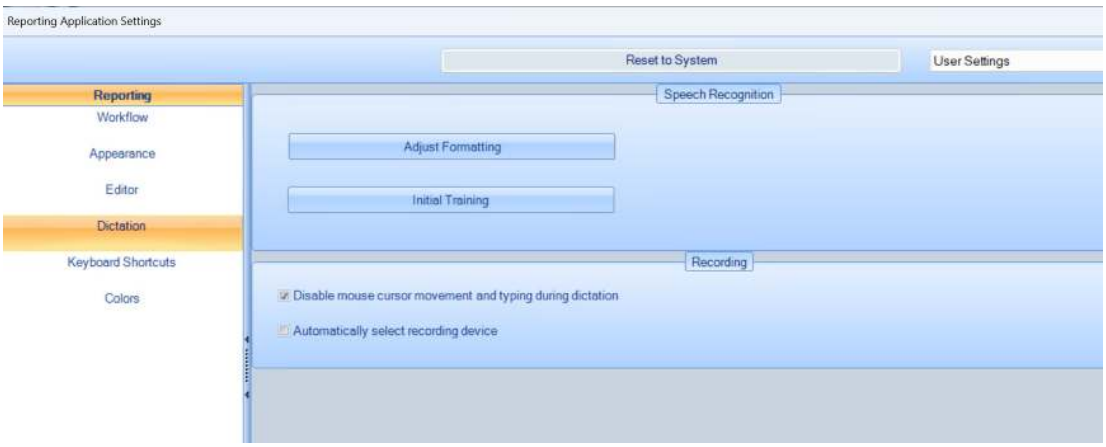
D000946129 Rev D/ * 2025-07-27

5 Applications Settings

5.1 Automatically select recording device

This features allows using multiple devices simultaneously, for example, using a headset for audio and Speechmike for navigation. If enabled, the recording device will switch to another device on button click on another device. If disabled, the recording device remains the same on button click on another device.

- From the **Reporting Application Setting**, check the box **Automatically select recording device**.



5.2 Disable mouse cursor movement and typing during dictation

This feature enables the user to enable or disable cursor movement during dictation.

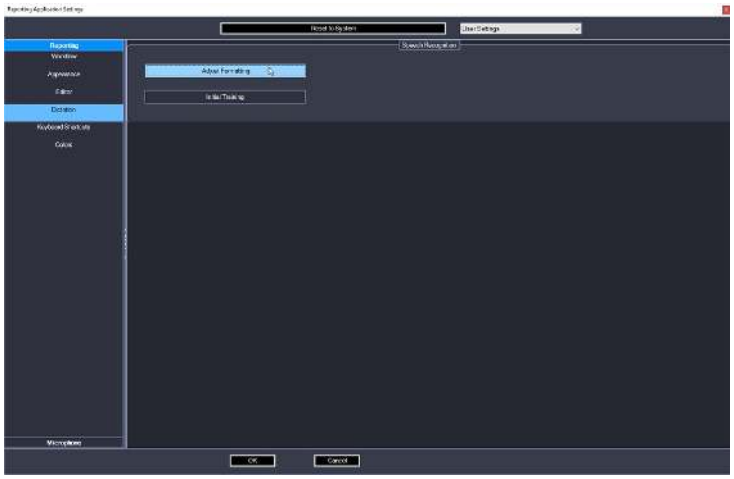
- From the **Reporting Application Setting**, check the box **Disable mouse cursor movement and typing during dictation.**

D000946129 Rev D/ * 2025-07-27

5.3 Adjust Formatting

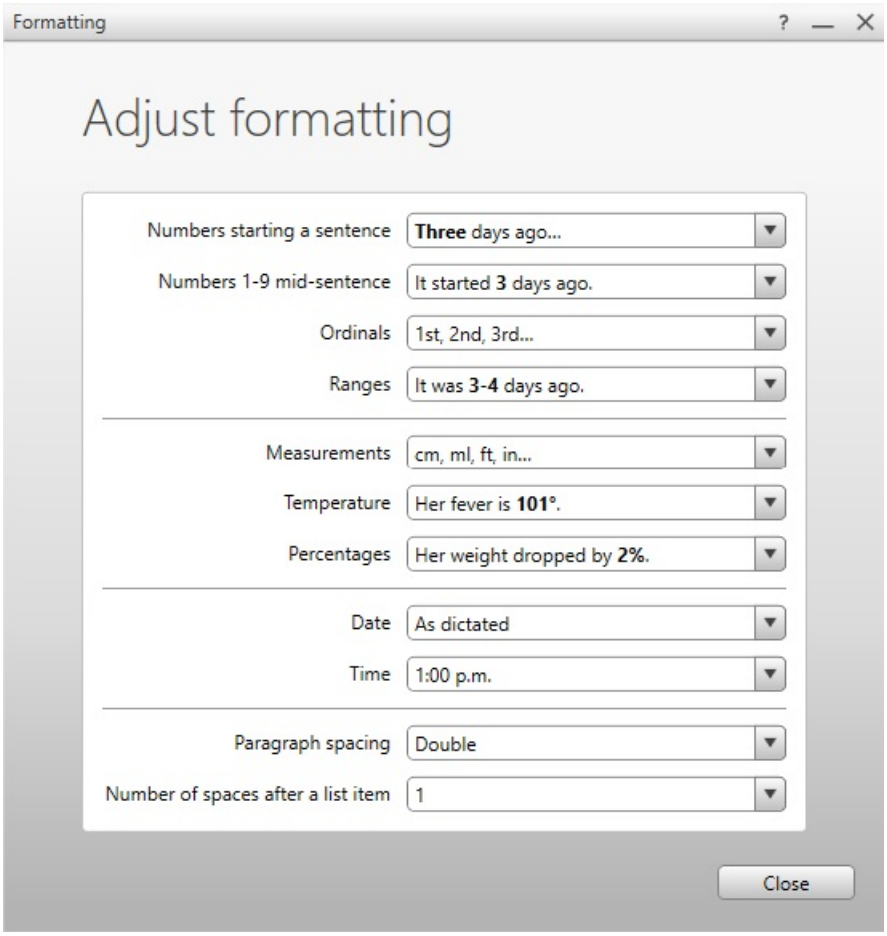
The **Adjust Formatting** option provides additional options related to the display of the dictated text.

- From the **Reporting Application Setting**, under **Dictation**, click **Adjust Formatting**.

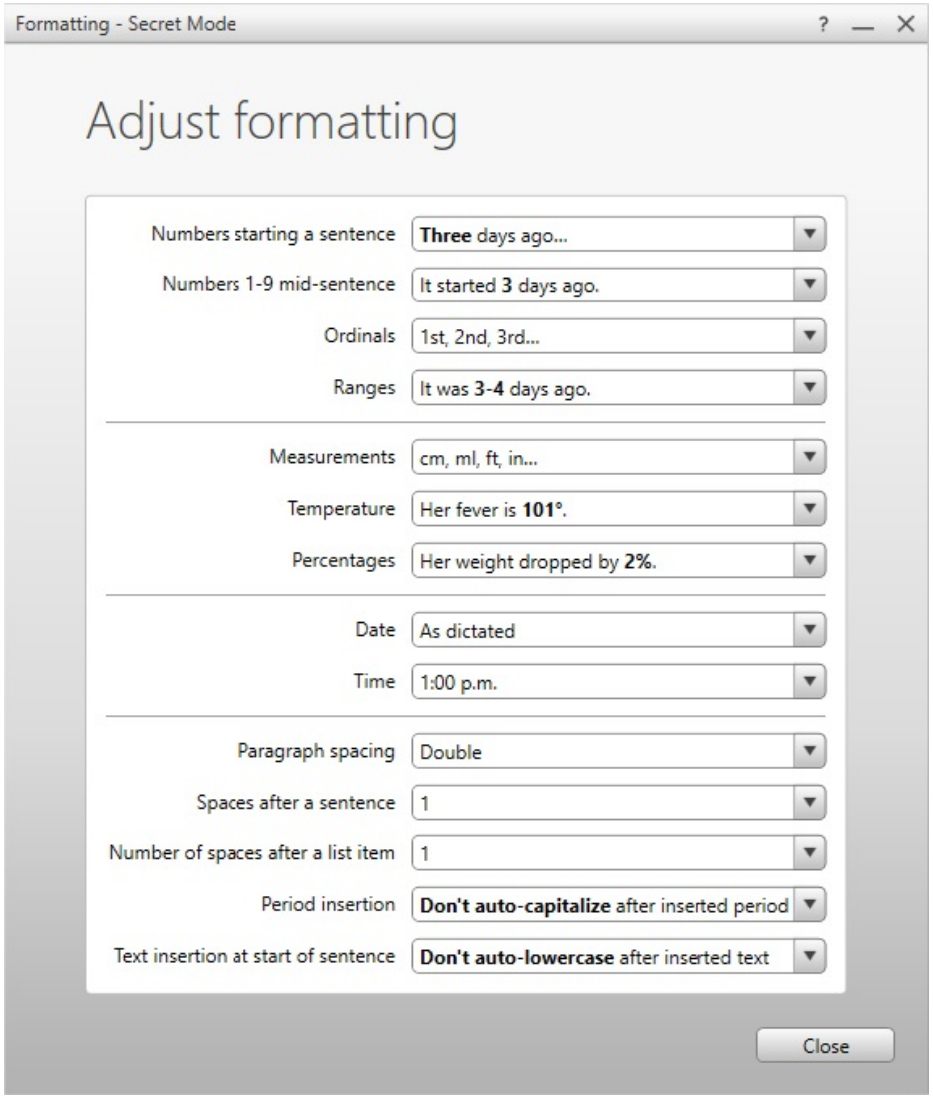


- The **Formatting** window displays, enabling you to format of Date, Time, measurements and other options according to your personal preferences.

D000946129 Rev D/ * 2025-07-27



- An **Advanced Formatting** window (i.e., Secret Mode) is available by holding the Shift-Key and clicking the dialog. Additional options will be available.



D000946129 Rev D/ * 2025-07-27

6 Voice Commands

For a list of all supported voice commands, see 6K9436 Vue PACS 12.2.8. Vue Reporting User Guide.

D000946129 Rev D/ * 2025-07-27

Philips

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

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

Australian Sponsor Details
Philips Electronics Australia Ltd.
65 Epping Road, North Ryde, NSW 2113,
Australia

Authorized Representative:

Wakil Diberi Kuasa:

Philips Malaysia Sdn. Berhad

196001000018 (3690-P)

Anchor Space 3 & 4

Co-labs Coworking

Level 11 Menara Ken TTDI

No 37 Jalan Burhanuddin Helmi

Taman Tun Dr Ismail

60000 Kuala Lumpur, Malaysia

Tel: 03-2054 9488

CE 0197

Registration No.: GB18651834218

No. Pendaftaran:

Printed in The Netherlands

D000946129 Rev D/ * 2025-07-27 - en-US