AW Server 3.2

Administrator Guide

CE 0459

5719555-1EN
Revision 7

Revision History

Revision	Date	Reason for change
1	2015–07	Initial release
2	2016–05	Updated with the following: • trademark attribution statements, • information about activating manual exam and series deletion, and importing/sharing preferences and assigning users to preference shares, • troubleshooting tip about Centricity™ RIS sessions in hybrid integration mode, • Single Photon Emission Computed Tomography (SPECT) exception removed.
3	2016–08	• CardEP added to the list of compatible applications • Troubleshooting tip about whitelisting executables amended • Note on scalability settings amended
4	2017–05	• Added notices on patient confidentiality • Added an overwrite option for manual preference import • Added a troubleshooting tip about launching Client Checker • Removed the list of available applications
5	2018–02	Updated with the following: • Smartcard authentication • integration with 3rd party DICOM hosts • DEPS-related privacy and security information • new options for scheduling image auto deletion • regulatory updates

(continued)

Revision	Date	Reason for change
6	2018-12	Updated with the following: • PostScript printing • audit trail (EAT) • selective preference sharing • preprocessing for 3rd party DICOM host integration • MSI installer improvement • privacy and security information • regulatory updates
7	2019-12	Updated with the following: • ***MailSender*** • symbols used in documentation • information on clipboard content • additional tags in DICOM host configuration

Contents

Page intentionally left blank

Chapter 1 Requirements and Regulatory Information

1.1 Regulatory requirements

This product complies with the regulatory requirements of the following:

- Council Directive 93/42/EEC concerning medical devices: the CE 0459 label affixed to the product testifies compliance to the Directive. First CE marked in 2015.

  For a system, the location of the CE marking label is described in the system manual.
- Medical Device Good Manufacturing Practice Manual issued by the FDA (Food and Drug Administration, Department of Health and Human Services, USA).
- International Electrotechnical Commission (IEC), international standards organization, when applicable.
- USA/HHS:

⚠ CAUTION

FEDERAL LAW RESTRICTS THIS DEVICE TO SALE BY OR ON THE ORDER OF A PHYSICIAN.

- GE Medical Systems SCS is ISO 9001 and ISO 13485 certified.
- The original document is written in English.

Manufacturer address:

GE Medical Systems SCS

283, rue de la Miniere

78530 Buc

FRANCE

Tel: +33 1 30 70 40 40

NOTE

The AW Server turnkey offering includes off-the-shelf server hardware. This server is not to be installed in the vicinity of patients, nor used in a patient environment. For more information regarding compliance with applicable regulations, refer to the documentation that came with your hardware components regarding compliance with applicable regulations.

1.2 Legal notices

GE and the GE Monogram are trademarks of General Electric Company.

Advantage Workstation, Advantage 4D, AdvantageSim, AutoBone, Centricity, Gemstone, Innova, InSite, OncoQuant, SmartScore, and VesselIQ are trademarks of General Electric Company or one of its subsidiaries.

Microsoft, Windows, the Windows logo, Windows Media, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Intel, Core, and Xeon are trademarks of Intel Corporation in the United States and/or other countries.

Parallels and Parallels Desktop are registered trademarks of Parallels Software International, Inc.

JavaScript is a trademark or registered trademark of Oracle and/or its affiliates in the U.S. and other countries.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

VMware, VMware vSphere and VMware vSphere Hypervisor are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

McAfee is trademark or registered trademark of McAfee, Inc. in the United States and other countries.

Trend Micro is trademark or registered trademark of Trend Micro Incorporated.

All other trademarks are the property of their respective owners.

AW Server 3.2 Administrator Guide is an independent publication and is not affiliated with, nor has it been authorized, sponsored, or otherwise approved by Microsoft Corporation.

AW Server 3.2 Administrator Guide is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc.

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

1.3 Software License - Intellectual Property

1.3.1 Preamble

Any software provided to the customer is subject to the specific license terms and conditions of the applicable agreement, or shrink-wrap, or click-wrap license. In the event of any conflict between those specific terms described below, the specific terms will supersede and prevail.

Generally those terms provided are as follows.

1.3.2 License Grant

GE grants to Customer a limited non-transferable license to use the Licensed Software subject to the limitations imposed under this Agreement and to the following:

The Customer shall use the Licensed Software only on the Equipment located at the Site and solely for the purpose of processing, storing, and transmitting images and data related to Customer's patients. Customer must obtain a supplementary license from GE (which GE may or may not grant, at its option) before using the Licensed Software (a) in connection with any equipment components other than the Equipment (except as expressly contemplated by this Agreement or any applicable Software documentation); (b) at any location other than the Site, or (c) to process, store, or transmit data related to patients other than Customer's patients.

Customer may make one copy of the Licensed Software in machine-readable form solely for backup purposes and shall reproduce on any such copy the copyright notice and any other proprietary legends that were on the original copy.

Customer shall comply with all restrictions on the use of Licensed Software that Customer is subject to as a licensee or sublicensee of GE under the terms of licenses or other agreements or arrangements with third parties.

1.3.3 Restrictions

Except as necessary for Customer to exercise its express rights hereunder, Customer may not itself or allow any third party to (i) make copies of the Licensed Software, (ii) distribute the Licensed Software to others, (iii) electronically transfer the Licensed Software from one computer to another over a network, or (iv) decompile, reverse engineer, disassemble, or otherwise reduce the Licensed Software to a human perceivable form. CUSTOMER MAY NOT MODIFY, ADAPT, TRANSLATE, RENT, LEASE, LOAN, RESELL FOR PROFIT, DISTRIBUTE, NETWORK, OR CREATE DERIVATIVE WORKS BASED UPON THE LICENSED SOFTWARE OR ANY PART THEREOF.

1.3.4 Ownership of Media

The media on which the Licensed Software is recorded or fixed is Customer's property. If Customer receives Licensed Software hereunder that renders Licensed Software that Customer has previously received redundant, Customer will return the redundant Licensed Software to GE or certify in writing that all copies of such Licensed Software have been erased.

1.4 User profile and training

1.4.1 Operator profile

As with any medical imaging process, only qualified personnel should use this equipment. You must be aware of the limitations of the basic imaging modality and of ensuing image processing. This includes understanding the limitations of the initial series acquisition, image processing technology used, and image display methods.

AW Server is intended to be used by physicians (any sub-specialty) and technologists trained to use a post processing review workstation. Interpretation of images may be done only by physicians trained in reading images of their corresponding modalities having knowledge of specific modality acquisition principles and quantitative analysis.

The users of the AW Server software application shall be a CT, MR, nuclear medicine, or radiology technologist, radiologist, cardiologist, or physician qualified with advanced applications training for software competencies or other personnel that the owner feels is properly trained for this software use (radiology assistant, physician assistant, etc.).

1.4.2 Training

There is no mandatory AW Server specific training. However, in order to avoid usage errors, the user MUST have a good knowledge and understanding of both the AW Server software and its primary operating functions. This can be accomplished through applications training and through the correct knowledge and application of Administrator Guide content.

Please contact your GE representative to order training for qualified individuals from your site. Make certain that the correct version of your operator manual is readily available at all times. Make a point to review the procedures and safety precautions periodically.

Before attempting to use the application, read the Safety and Regulatory Information. It describes safety and regulatory information that you must thoroughly understand before you begin to use the software.

AW Server provides post processing capabilities to its clients. Any data acquired on a variety of diagnostic imaging devices can be processed using AW Server (with the exception of x-ray mammography).

AW Server can be used for the medical purposes described in Indications for Use (see Indications for Use). There is no limitation concerning patient population, the body or type of tissue, or the frequency of use.

1.5 System requirements

NOTE

For detailed information, refer to the AW Server 3.2 Advanced Service Manual.

1.5.1 AW Server hardware specifications

The following specifies the AW Server hardware requirements.

Item	High Tier	Low Tier
CPU	• 4 x Intel® Xeon® x7542 (2.6GHz/6-Core/18MB/130W) Processors or • 4 x Intel Xeon E5-4620 v2 (2.6GHz/8-Core/20MB/95W) Processors	• 2 x Intel Xeon x5650 (2.66GHz/6-Core/12MB/95W) Processors or • 2 x Intel Xeon E5-2630 v2 (2.6GHz/6-Core/15MB/80W) Processors
RAM	• For x7542 CPU: 64GB PC3-10600R DDR3 ECC DIMM (32 x 2GB, Improved Hemisphere) • For E5-4620 v2 CPU: 64GB DDR3 1600MHz or higher ECC DIMM (16 x 4GB, 1 DIMM per channel) or 256GB DDR3 1600MHz or higher ECC DIMM (16 x 16GB)	• For x5650 CPU: 24GB DDR3 ECC DIMM (6 x 4GB, 1Rx4 PC3-14900-11 Kit, 1600MHz or higher 1 DIMM per channel) • For E5-2630 v2 CPU: 24GB DDR3 1600MHz ECC DIMM (6x4GB) or 64GB DDR3 1866MHz ECC DIMM (8 x 8GB)
HDD	Internal: • 2 x 146GB SAS 15000 RPM HDD • SAS RAID controller card, P420i with 512MB FBWC External (in an additional 2U chassis): • 12 x 1TB SAS 7200 RPM • SAS RAID controller card, P421 with 1024MB FBWC	Internal: 6 x Internal HP® 500GB 6G SATA 7.2k 2.5” SC MDL HDD External: none
PCI Express Expansion	• Has to include at least four (4) PCI Express expansion slots • The slots shall be capable of accommodating at least low-profile cards	—
Service	Embedded Service Processor Card	Embedded Service Processor Card

In a **virtualized environment**, the following minimum resources are required for:

Low Tier

- a **virtualization server** (host):
  - Intel Xeon CPUs supporting SSE 4.1 instructions
  - 8 physical CPU cores (using hyperthreading and CPU overcommit is not recommended)
  - 1 Ethernet port (minimum 1Gb/s)
  - data store to store all Virtual Machine (VM) data with thick provisioning

  - enough RAM to meet VM RAM requirements without RAM overcommit

- a **guest** (hosted) OS to run an AW Server Node:
  - **CPU**: 8 vCPUs
  - **HDD**: 70GB virtual HDD, configured disks for OS: 2
  - **RAM**: 24GB
  - **NIC**: 2 x Ethernet

- **High Tier**
- a **virtualization server** (host):
  - Intel Xeon CPUs supporting SSE 4.1 instructions
  - 24 physical CPU cores (using hyperthreading and CPU overcommit is not recommended)
  - 1 Ethernet port (minimum 1Gb/s)
  - data store to store all Virtual Machine (VM) data with thick provisioning
  - enough RAM to meet VM RAM requirements without RAM overcommit

- a **guest** (hosted) OS to run an AW Server Node:
  - **CPU**: 24 vCPUs
  - **HDD**: 70GB virtual HDD, configured disks for OS: 2 in no integration and hybrid integration, 1 in seamless integration mode
  - **RAM**: 64GB
  - **NIC**: 2 x Ethernet

Supported **VMware vSphere Hypervisor** environments: 5.1, 5.5, and 6.0.

1.5.2 AW Server client requirements

The following section specifies the minimum client hardware requirement. The end user client hardware shall meet or exceed these specifications.

Item	Specification
Processor	Intel Core™ 2 Duo @2.33GHz or Pentium® 4 @3GHz minimum (or equivalent)
Memory	1GB minimum
Disk drive	250MB free space available
Network card	100Mb/s minimum, 1Gb/s recommended
Screen Resolution	Minimum: 1024H x 768V with full color (32 bit) Optimal: 1280H x 1024V or 1600 x 1200 Up to 6 MP for optimal performance.

(continued)

Item	Specification
Mouse	Two or three-button mouse. Three button mouse is recommended for best use of functions.
Browser Security Settings	JavaScript™ enabled

1.5.3 Required system – software environment

1.5.3.1 Client Operating system

- Parallels Desktop® 10 for Mac (Mac OS® 10.10, Windows® 8.1 32bit, 64bit)
- Windows® 7 SP1 32bit, 64bit
- Windows® 8.1 32bit, 64bit

1.5.3.2 Boundary Values

Image processing capabilities are limited by the hardware and the license type purchased by the customer. Licensing is based on slice count and when the number of slices that are being processed simultaneously approaches the limits defined for the purchased license type, users may experience slower than normal performance.

1.5.4 Security

NOTE

> Some security software programs could potentially block the installation of the AW Server client software or impact the connectivity to the server. If you are having trouble, you may want to temporarily disable those programs or set the AW Server web site status to "trusted."

1.5.5 Software

NOTE

> Other non-GE software applications and operating system options, such as antivirus, VPN, firewall and network-intensive applications, running on devices used as AW Server clients may impair the performance and effectiveness of the product. Do not use the software if it is damaged or compromised. If you in any way suspect that its integrity has been compromised, contact your customer service representative immediately.

Page intentionally left blank

Chapter 2 About this Guide

2.1 About this guide

Depending on user privileges, AW Server users may belong to one or more of the following categories:

- **Limited users**: A user (e.g., a referring physician) with restricted access to patient database and applications. A limited user has to provide at least two of the following criteria to perform a successful search: patient name, patient ID and birthdate. A limited user:
    - cannot export DICOM data,
    - has no access to Service Tools,
    - cannot import preferences,
    - cannot delete exams and/or series from the ***Worklist Browser***,
    - cannot browse or search remote host worklists,
    - cannot access, create, rename, or delete referral worklists.
- **Standard users**: A CT, MR, nuclear medicine, or radiology technologist, radiologist, cardiologist, or physician qualified with advanced applications training for software competencies or other personnel that the owner feels is properly trained for this software use (radiology assistant, physician assistant, etc.).
- **Administrator users**: A person who manages the computer system within an organization. In larger organizations this could be someone in your IT department. In smaller organizations (such as stand alone sites), this could be a user who has been designated as the administrator.
- **Service users**: A GE Field Engineer who has full access to the system to manage and maintain it.

This guide is for AW Server users with administrator user privileges. It does not identify components or features that are standard or purchasable options. Therefore, if a feature or component noted in this documentation is not on your system, it is either not available on your system configuration or your site has not purchased the option.

If necessary, consult the relevant operator manuals to familiarize yourself fully with the application, the use of the various controls, menus and windows, and terminology before continuing.

For general user information, refer to the AW Server 3.2 User Guide.

NOTE

> To view applications documentation, Adobe® Reader® X or later is required. To download Adobe Reader, please visit Adobe System's website at www.adobe.com.

2.1.1 Additional manuals

Software options can be ordered for AW Server 3.2. In this case, a specific operator manual will be delivered to you with specific information on operating the software applications.

This online help is only one part of a larger set of documentation available. Additional manuals include those applicable to the advanced applications. If necessary, consult the relevant operator manuals to familiarize yourself fully with the application, the use of the various controls, menus and windows, and terminology before continuing.

These manuals can be accessed via the web or the tools icon (see Viewing user manuals).

2.1.2 Safety information

The safety topics contain warnings and cautions related to the AW Server and describe the safety information you must understand thoroughly before you begin to use the system. If you need additional training, seek assistance from qualified GE personnel.

The equipment is intended for use by qualified personnel only.

It is important for you to periodically review the procedures and safety precautions. **It is important to read and understand the contents of this guide before attempting to use this product.**

2.1.3 Purpose of this guide

This manual is written for health care professionals to provide the necessary information relating to the proper operation of this system.

2.1.4 User interface note

Please note that the screen captures in this document are intended for demonstration purposes only and may not always be fully identical to the actual user interface (e.g., in color scheme). Use these screen captures as guides.

Chapter 3 Product Description

3.1 Product description

AW Server is a medical software system that allows multiple users to remotely access AW applications from compatible computers on a network. The system allows networking, selection, processing and filming of multimodality DICOM images.

Both the client and server software are only for use with off the shelf hardware technology that meets defined minimum specifications.

The device is not intended for diagnosis of mammography images. The device is not intended for diagnosis of lossy compressed images. For other images, trained physicians may use the images as a basis for diagnosis upon ensuring that monitor quality, ambient light conditions and image compression ratios are consistent with clinical application.

AW Server is a software package, which may be purchased as a turnkey solution that includes off-the-shelf enterprise-class server hardware that allows easy selection, review, processing and filming of multiple modalities DICOM images from a variety of PC client machines, using LAN networks. It also allows user selectable compression schemes for transferring medical images.

As an option the server can be installed on a virtual hardware.

AW Server is intended to be used in a manner similar to the current GE AW workstation product. It will be used to create and review diagnostic evidence related to radiology procedures by trained physicians in General Purpose Radiology, Oncology, Cardiology and Neurology clinical areas.

AW Server may be used with a variety of other GE software medical devices, which are cleared by appropriate regulatory bodies in their own names.

Page intentionally left blank

Chapter 4 Safety

4.1 Introduction

To ensure efficient and safe use of the AW Server it is essential to read this Safety section and all associated topics before attempting to use the software. The Safety section contains important information for the safe and effective use of the AW Server.

To use the AW Server, the user MUST have a good knowledge of the AW Server applications. The software is intended for use by qualified and trained personnel only. If you need additional training on any AW Server application, seek assistance from your GE applications specialist.

Make certain that the correct version of your operator manuals are readily available at all times. Make a point to review the procedures and safety precautions periodically.

Safety note legends:

⚠ **⚠ WARNING**

THIS INDICATES A POTENTIALLY HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, COULD RESULT IN DEATH OR SERIOUS INJURY.

⚠ **⚠ CAUTION**

THIS INDICATES A POTENTIALLY HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, MAY RESULT IN MINOR OR MODERATE INJURY.

Non-safety note legend:

❗ ***NOTICE***

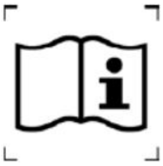
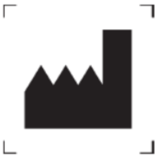
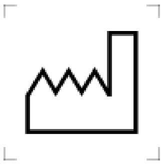
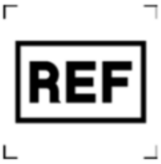
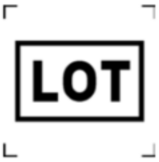
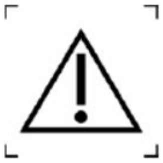
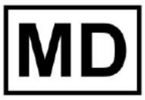
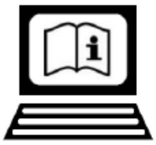
This indicates a non–hazardous situation which, if not avoided, could result in equipment damage, lost time, or reduced image quality.

Note:

NOTE

Provides additional information that is helpful to you. It may emphasize certain information regarding special tools or techniques, items to check before proceeding, or factors to consider about a concept.

4.2 Symbols used in documentation

Symbol	Description
	**Consult Instructions for Use**: Indicates that the user shall read Instructions for Use.
	**Manufacturer**: Indicates the medical device manufacturer's name and address.
	**Date of manufacture**: Indicates the date when the medical device was manufactured.
	**Catalogue number**: Indicates the manufacturer's catalogue number so that the medical device can be identified.
	**Batch code**: Indicates the manufacturer's batch code so that a specific medical device can be identified.
	**General caution**: Used to highlight the fact that there are specific warnings or precautions associated with the application, which are not otherwise found on the label.
	**Medical Device**: Indicates this product is a medical device.
	**Electronic Instructions for Use (e-IfU)**: Indicates this device is delivered with electronic instructions for use.

4.3 Indications for Use

AW Server is a medical software system that allows multiple users to remotely access AW applications from compatible computers on a network. The system allows networking, selection, processing and filming of multimodality DICOM images.

Both the client and server software are only for use with off the shelf hardware technology that meets defined minimum specifications.

The device is not intended for diagnosis of mammography images. The device is not intended for diagnosis of lossy compressed images. For other images, trained physicians may use the images as a basis for diagnosis upon ensuring that monitor quality, ambient light conditions and image compression ratios are consistent with clinical application.

4.4 Accuracy

⚠ **WARNING**

ALWAYS ENSURE THAT THE DISPLAYED IMAGES BELONG TO THE APPROPRIATE PATIENT WITH THE ORIGINAL ACQUISITION PARAMETERS. (1)

⚠ **WARNING**

ALWAYS CHECK THAT THE GEOMETRY AND ACQUISITION PARAMETERS DISPLAYED FOR AN IMAGE ARE COMPLIANT WITH THE ACQUISITION SYSTEM DISPLAY. (3)

⚠ **WARNING**

ONLY USE DATES WITH A FOUR-DIGIT YEAR AND A THREE-CHARACTER MONTH. NOTE THAT DATES ARE ALWAYS IN ENGLISH. (9)

4.5 Data storage

⚠ **WARNING**

WHEN DOWNLOADING DATA FROM THE SERVER TO THE LOCAL CLIENT:

- DO NOT OVERWRITE EXISTING FILES OR DIRECTORIES.
- ALWAYS CHECK THAT DATA DOWNLOADED FROM SERVER TO THE LOCAL CLIENT ARE APPROPRIATE BEFORE USING FOR ANY PURPOSE.
- DO NOT USE IMAGES PRINTED ON A NON-DICOM PRINTER FOR DIAGNOSIS.
- DO NOT ATTEMPT TO USE OR ACCESS ANY TEMPORARY DATA CREATED WHEN SAVING A FILE OR DIRECTORY. (16)

❗ ***NOTICE***

AW Server is not a storage commitment or an archive device for medical imaging data. All data on the AW Server is transient. A secure copy should be maintained in a separate location such as a PACS archive, original acquisition device, or long-term archive media.

4.6 Display and window/level

4.6.1 Display

NOTE

The image display quality is limited by the display device of the client hardware. The medical imaging professional operator is required to use good judgement of the display quality, ambient lighting conditions and other factors to decide if the presentation is of sufficient quality for the clinical circumstances. AW Server client software presents information using color and is not intended for use on gray scale monitors.

NOTE

The client size is above the supported value. Please note that you may encounter some serious performance degradation.

NOTE

The client size is above the recommended value. Please note that you may encounter performance degradation.

4.6.2 Image Compression

NOTICE

The image quality may be degraded by the data compression techniques (depending on the compression settings). Diagnosis has to be performed on the original images in DICOM format.

4.7 Filming, saving, and data export

4.7.1 Filming and saving

NOTICE

The image quality may be degraded by the data compression techniques (depending on the compression settings). Diagnosis has to be performed on the original images in DICOM format.

4.7.2 Data Export

The Data Export function allows you to export images (in the form of an “electronic film”) to other systems that do not support the DICOM format.

⚠ **WARNING**

THE MPEG/AVI/MOV MOVIES COMPRESSED WITH HIGH IMAGE QUALITY MAY NOT BE PLAYED BACK CORRECTLY ON SLOWER MACHINES. IMAGE SKIPPING MAY OCCUR. (38)

NOTICE

The image quality may be degraded by the data compression techniques (depending on the compression settings). Diagnosis has to be performed on the original images in DICOM format.

4.7.3 MailSender

⚠ WARNING

THE SEND BY EMAIL FUNCTIONALITY IS INTENDED TO HELP FACILITATE COMMUNICATION BETWEEN CLINICIANS. PATIENT MANAGEMENT SHOULD NOT BE DEPENDENT ON RECEIPT OF EMAIL COMMUNICATION.

⚠ WARNING

EMAIL CONTENT CONTAINS LIMITED PHI SUCH AS A UNIQUE EXAM IDENTIFIER AND TIME OF SCAN.

⚠ WARNING

FOR SECURITY REASONS, USE OF PLAIN SMTP MAIL SENDING IS HIGHLY DISCOURAGED. USING A TLS SERVICE IS STRONGLY ADVISED FOR SECURITY PURPOSES.

⚠ WARNING

IT REMAINS THE RESPONSIBILITY OF THE USER TO CONFIGURE THE SEND BY EMAIL FUNCTIONALITY WITH A SECURE MAIL SERVER AND ENSURE COMPLIANCE WITH REGULATIONS FOR EMAIL DELIVERY TO IT ADMINISTRATIVE CONFIGURED RECIPIENTS.

4.8 Image reliability, quality, and resolution

4.8.1 Image compression

⚠ WARNING

LOSSY DATA COMPRESSION IS AVAILABLE ON THE AW SERVER TO HELP IMPROVE THE DISPLAY PERFORMANCE OF THE APPLICATIONS. THE JUDGEMENT OF THE MEDICAL IMAGING PROFESSIONAL IS AN IMPORTANT PART OF REACHING THE APPROPRIATE CONCLUSION FROM THE RESULTS PRESENTED BY COMPRESSED IMAGES. IF NECESSARY, TURN COMPRESSION OFF BEFORE USING IMAGES FOR DIAGNOSIS. (18)

4.8.2 Image resolution

The image set resolution is determined by:

- the size of the field-of-view
- the matrix size
- the inter-slice distance

In the acquisition plane, the measurement accuracy cannot be better than the size of the smallest element. In the same way, the accuracy in a direction perpendicular to the acquisition plane cannot be better than the inter-slice distance. In the acquisition plane, for a field-of-view of about 25cm, the smallest detail in an image acquired with a 512x512 matrix will be about 0.5x0.5mm. With a 256x256 matrix, the smallest detail will be 1x1mm.

4.9 Installation

⚠ **WARNING**

THE CLIENT MONITORS SHALL BE POSITIONED SO AS TO AVOID REFLECTIONS FROM ROOM LIGHTING OR WINDOWS, OR TOO MUCH AMBIENT LIGHT STRIKING THE MONITOR SCREEN DIRECTLY. INCORRECT POSITIONING MAY LEAD TO DEGRADED IMAGE QUALITY AND CRITICAL FEATURES ON THE IMAGES NOT BEING CLEARLY VISIBLE. (47)

NOTE

Always run the image quality tool when you change your monitor, graphic card or monitor cable, or when you dock or undock a laptop, or change viewing conditions – for example taking a laptop into or out of a dark reading room.

NOTICE

Federal law restricts this device to sale by or on the order of a physician.

4.10 Measurement

This section provides information about the accuracy of on-view measurements. This accuracy depends on various factors, and in particular on the size of the region of interest (ROI) being measured.

NOTE

In the 2D and 3D Viewers, the ROI statistics will vary slightly depending on the zoom factor used to view the images when the ROI is deposited. If exact accuracy of the mean and standard deviation is critical, make sure the image is not zoomed before depositing the ROI.

To assess the accuracy of measurements performed with other AW Server applications, please consult the Measurements section of the appropriate user manuals.

4.11 Non-GE images

Follow the DICOM acquisition parameter guidelines listed in each application user guide.

Consult GE-published DICOM conformance statement of AW Server 3.2 and the application package used.

4.12 PACS and 3rd party integration

⚠ WARNING

IN PACS INTEGRATION, THERE MAY BE A TIME DELAY BETWEEN THE TIME THE USER SAVES DATA FROM AN AW APPLICATION TO THE TIME IT CAN BE SEEN IN THE PACS WORKLIST. (56)

⚠ WARNING

IN THE CASE OF PACS INTEGRATION, IF THE NETWORK BETWEEN THE PACS AND THE AW SERVER IS LOST THE PATIENT IMAGE DATA READ AND APPLICATION START IS NOT POSSIBLE. (57)

⚠ WARNING

IN THE CASE OF COMMAND LINE INTEGRATION WITH A 3RD PARTY SYSTEM, LOADING A NEW PATIENT AND STARTING A NEW APPLICATION ON THE 3RD PARTY SYSTEM DOES NOT AUTOMATICALLY UPDATE THE DATA DISPLAYED ON THE AW SERVER. THIS WILL CAUSE DIFFERENT PATIENTS TO BE DISPLAYED ON THE DIFFERENT MONITORS.TO SYNCHRONIZE THE PATIENTS BETWEEN THE TWO MONITORS, USERS MUST CLOSE THE OPEN APPLICATION ON THE AW SERVER, DISPLAY THE PATIENT BROWSER, AND RE-INVOKE AW SERVER CLIENT ON THE 3RD PARTY SYSTEM. (110)

4.13 Quality assurance and performance

⚠ WARNING

TO ENSURE CONSISTENT IMAGE QUALITY FROM THE AW SERVER CLIENT WORKSTATION, IT IS THE USER'S RESPONSIBILITY TO IMPLEMENT A PROCEDURE OF REGULAR QUALITY ASSURANCE CHECKS. (69)

4.13.1 Client checker

WARNING

THIS TOOL IS DESIGNED TO EVALUATE YOUR CLIENT CONFIGURATION AND MONITOR TO HELP YOU DETERMINE IF YOUR SYSTEM IS SUFFICIENT FOR THE CLINICAL APPLICATION AW SERVER. THIS QUALITY CHECK IS AN INITIAL EVALUATION OF YOUR OPERATING SYSTEM. IT IS NOT MEANT TO REPLACE YOUR QA PROCEDURES. (70)

WARNING

ALWAYS RUN THIS IMAGE QUALITY TOOL WHEN YOU CHANGE YOUR MONITOR, GRAPHIC CARD OR MONITOR CABLE, OR WHEN YOU DOCK OR UNDOCK A LAPTOP, OR CHANGE VIEWING CONDITIONS – FOR EXAMPLE TAKING A LAPTOP INTO OR OUT OF A DARK READING ROOM. (71)

4.13.2 Performance

For AW Server installations on GE-provided server hardware or on customer provided VMware® computing capacity is limited by the hardware resources. In order not to overload the system, a slice count mechanism is used. When the number of slices that are being processed simultaneously approaches the applicable limits, users may experience slower than normal performance.

WARNING

THERE MAY BE A PERFORMANCE DEGRADATION AS THE NUMBER OF USERS ON THE AW SERVER INCREASES. (72)

WARNING

THE PROCESSING EFFICIENCY AND SPEED OF THE AW SERVER ARE AFFECTED BY THE AMOUNT OF MEMORY AND THE NUMBER OF ACTIVE PROCESSES RUNNING ON THE CLIENT. CONVERSELY, RUNNING THE AW SERVER CLIENT MAY TEMPORARILY IMPACT OTHER ACTIVE PROCESSES. (89)

⚠ **WARNING**

WHEN RUNNING AW SERVER ON A HOME NETWORK, EXTERNAL SOFTWARE SUCH AS CITRIX AND VPN MAY COMPRESS DATA DURING DATA TRANSFER BETWEEN THE AW SERVER AND YOUR CLIENT. IN THIS CASE, THE IMAGE QUALITY MAY BE IMPACTED AND THESE IMAGES MUST NOT BE USED FOR DIAGNOSIS. (90)

⚠ **WARNING**

IF THE SERVER IS NOT IN A CONTROLLED ACCESS ENVIRONMENT, THE SERVER COULD BE SHUTDOWN AT ANY TIME WITHOUT GOING THROUGH AN ORDERLY SHUTDOWN PROCEDURE. ALTHOUGH NOT REQUIRED, CONTROLLED ACCESS IS STRONGLY RECOMMENDED FOR ALL AW SERVERS. (91)

4.14 Safety related software messages

Messages giving information and warnings relating to the current system status are displayed while using the AW Server. Some of these messages may be related to safety issues. For example, a message may warn that a screen or printed image will be enlarged or reduced, and this must be taken into consideration when making a diagnosis. It is important that users take note of and act on the information given in these messages. The table below shows safety–related messages which may be displayed. In manuals intended for use in countries in which the on–screen language is different from the local language, the table shows the displayed messages and gives a translation in the local language. In manuals intended for use in countries in which the on–screen language is available in the local language, the right side of the table is blank.

English	Translation
Print not for diagnosis (98)	
System could not supply enough resources. (106)	
Please be aware that the images contained in this electronic film may have lost information due to a lossy compression, and are not for diagnostic use. Please note that the MPEG/AVI/MOV movies compressed with high image quality may not be played back correctly on slower machines - image skipping may occur. (109)	

Chapter 5 Privacy and Security Information

5.1 Access controls

5.1.1 Remote device access

The AW Server system provides access control for individual users on a unique system or cluster.

The AW Server system does not provide access based on additional parameters like:

- System or modality type identifier, specific customer.
- Specific customer site, physical location country which is available when the user provides a Virtual Private Network (VPN) access.

5.1.2 Account management

5.1.2.1 Removal of temporary/emergency accounts

The AW Server system does not provide the capability to create specific temporary or emergency accounts.

5.1.2.2 Disabling inactive accounts

The AW Server system does not automatically deactivate inactive local user accounts.

The customer can enable the AW Server Enterprise authentication to manage the appropriate site authentication policy.

5.1.2.3 Automated audit actions

The AW Server system will log account creation, modification, enabling, disabling, and removal actions, but will not provide any notification to specific user.

5.1.2.4 Access revocation

The AW Server does not provide an access authorization revocation feature resulting from changes to the security attributes of subjects and objects based on customer defined rules. The IT admin is responsible to revoke user access directly on AW Server for local users and on hospital’s Authentication Server.

5.1.3 Access enforcement

Standard users will access the whole worklist of patients - except for certain integration modes.

Limited access users will not have access to the worklist.

The AW Server system does not support context based authorization that will offer features like:

- Time-of-Day restrictions,
- weekly schedule restrictions,

- workstation (location) restrictions,
- patient consent restrictions,
- specific fields to trigger data restrictions,
- warnings related to access level restrictions.

The AW Server has a limit on the maximum number of concurrent sessions which is not specific to an account.

5.1.4 Information flow enforcement

The user has to ensure that s/he has the appropriate authorization to import images from the ***Free Image Importer*** tool or export data using RMP feature, DICOM Media Creator or Service Tools.

The AW Server does not support secure DICOM communication.

Communication between the AW Server and printer devices is not encrypted.

5.1.5 Unsuccessful login attempts

The AW Server local account management is able to lock an account for a configurable time after a configurable number of login failures.

5.1.6 System use notification

The AW Server does not offer a specific capability to configure a notification message displayed to all users before granting access to the system.

5.1.7 Session lock

AW Server offers a configurable client timeout that is not available in case of PACS integration.

The client timeout is configured for all clients and cannot be configured per client. When client timeout is triggered the user is logged out.

In all cases, the user has to configure the operating system session lock on his/her own client.

5.1.8 Remote access

It is the customer's responsibility to provide an encrypted VPN - or another access mechanism - if access is needed outside of the hospital.

5.1.8.1 Automated monitoring/control

AW Server does not provide an interface or an automated mechanism to monitor user access.

Such information is stored in specific log files that can be provided upon request.

5.1.8.2 Privileged commands/access

AW Server InSite™ Service connectivity allows GE to access the system remotely.

The access to Terminal tool requires password authentication.

The AW Server does not display any notification for the user when remote connectivity is established or closed.

5.2 Audit and accountability

5.2.1 Content of audit records/additional audit information

The AW Server provides the following audit events:

- user client login,
- access to data,
- deletion of data,
  and
- export of data

along with date and time, source or destination, identity of the user and identity of the subject when applicable.

The audit logs cannot be extended or configured.

The information system does not provide centralized management and configuration of the content to be captured in audit records.

The information system does not provide alerts nor customizable actions in case of an audit processing failure.

The product does not provide the capability to automatically process audit records.

The product does not provide cryptographic mechanism to protect integrity of information or audit tools.

5.2.2 Audit review, analysis and reporting

Audit events can be exported to external servers for a future usage by the hospital organization.

5.2.3 Protection of audit information, audit backup/retention

Audit records are not backed up.

Audit logs can be stored locally – in which case log rotation protects against filling up AW Server disk partition – or can be exported to configured external audit repository servers.

5.2.4 Accounting of disclosures - capability

The AW Server audits the access to a specific case and export to some remote devices.

It is the user's responsibility to analyze such reports using Service Tools.

5.3 Identification and authentication

5.3.1 Standards

AW Server can be configured to use central user authentication from the hospital.

5.3.2 Network access to privileged accounts

No multifactor authentication is available to access accounts.

5.3.3 Network access to privileged accounts - replay resistant

The AW Server does not define a customizable replay-resistant authentication mechanism.

5.3.4 Device-to-device/health information

The AW Server does not provide control of sources of personal identification. By default, all incoming DICOM data is accepted.

The AW Server does not authenticate remote devices (printers, remote DICOM hosts).

5.3.5 Authenticator management

When creating a local account, the AW Server:

- enforces a minimum password length,
- does not force for specific combination of characters to increase the password complexity,
- does not force a new password to be different from the previous one,
- does not provide password limited lifetime,
- does not prevent to reuse the same password for another user,
- does not implement temporary password for system login.

5.3.6 Login history

The AW Server does not support a configurable message containing the last successful login date and time to be displayed at successful login.

5.4 System and communications protection

5.4.1 Security function isolation

The AW Server does not implement kernel code. It restricts access through user authentication and isolate kernel, application and user function by setting appropriate file permissions to files.

The AW Server does not support the verification of the correct operation of security functions, neither the automatic notification to administrator defined personnel.

5.4.2 Information in shared resources

Once logged in, standard users have access to configured export functionalities and the system does not provide rules to prevent specific transfer via the configured shared resources.

5.4.3 Denial of service protection

The AW Server does not provide specific protection against denial of service attacks. The AW Server has to be used only in a hospital environment protected from remote attacks by the hospital network.

5.4.4 Boundary protection

The network security is under the responsibility of the user's organization.

It is the hospital's responsibility to ensure that (mobile) devices connecting to the AW Server do not authorize split tunneling. In particular, if the hospital provides a VPN to access the hospital network from outside, it is recommended to turn off split tunneling on such devices.

5.4.5 Cryptographic protection

The AW Server supports HTTPS communication, but does not allow customizable organization-defined cryptographic usage.

5.4.6 Secure name/address resolution service

The AW Server system uses name/address resolution service coming from:

- information configured in file /etc/hosts,
- primary and secondary DNS servers provided by the organization if any.

The AW Server does not implement DNS security features and does not provide additional data origin and integrity artifacts along with the authoritative name resolution data the system returns.

5.4.7 Process isolation

The AW Server information system does not implement separate execution domain for each executing process.

5.4.8 Malicious code protection

The AW Server antivirus allows detecting malicious code. The removal of such code has to be done manually.

5.5 System and information integrity

The AW Server does not provide tools to monitor inbound and outbound communications traffic or to alert in case of unusual activities or conditions.

The AW Server does not provide tools to verify user defined security functions.

The AW Server does not encrypt the data at rest.

5.6 Minimization of personally identifiable information

During clinical diagnosis the Patient Name is displayed on the AW Server client PC monitor.

The Patient Names stored on AW Server might be also visible for authorized service personnel and product administrator. They have deletion rights on locally stored patient data.

When a service contract is valid and the system is connected via GE, some data necessary for GE service may be transferred to GE back office.

5.7 Safety mode

The AW Server does not support the Emergency Mode meaning the support for a continuous patient treatment for a predefined period of time.

5.8 Patient confidentiality

DICOM

NOTICE

DICOM communications are not inherently secure. AW Server recommends protection of sensitive data be controlled by the site security policy.

Data Export

NOTICE

Data Export does not apply encryption on exported data for generic interoperability. Protection of sensitive data shall be controlled by the site security policy.

NOTE

Copying images to the clipboard will also copy the patient name if it is displayed on the images. If patient privacy is required, be sure to remove patient information before printing or saving.

NOTE

AW Server should always be run over the hospital VPN (virtual private network) if accessing from any external network. Running it on the open internet without proper network security measures (such as enterprise firewall) could lead to patient privacy issues.

NOTE

> The AW Server includes hard disk drives which may hold medical data related to patients. Such equipment may in some countries be subject to regulations concerning the processing of personal data and the free circulation of such data. It is strongly recommended that access to patient files be protected from all persons not in medical attendance.

To prevent unauthorized access to patient data:

When leaving the client station unattended for any length of time, exit the AW Server applications and close your user session.

Page intentionally left blank

Chapter 6 Getting Started

6.1 Introduction to AW Server

6.1.1 Introduction to AW Server

AW Server may act as a collaborative workflow connection between clinicians within the department and between the department and referring physicians. AW Server is a central access point for Diagnostic Imaging exams, even those in progress, allowing clinicians to collaborate. From any supported PC, a clinician can use AW Server to export diagnostic images into other desktop applications.

The AW Server may also serve as a computational engine powering advanced applications. AW Server may be purchased as a turnkey solution that includes off-the-shelf enterprise-class server hardware or installed in a hardware virtualization environment.

Interactive workflows include user interaction with applications either selected in the worklist, or selected by the user with help from the AW Server software. Multiple users can manipulate or view a data set at the same time, facilitating collaboration.

This manual contains information specific to the AW Server. It does not contain information on any client operating system.

AW Server terminology

When talking about the AW Server product, two major terms are used to describe the components:

- The **server**: the hardware and software applications (supplied by GE) and exam data and can be used simultaneously by multiple people from multiple locations.
- The **client**: the hardware an individual uses to access the server to run applications and access data on the server. The client is typically a personal computer, laptop, PACS, etc. and can be located practically anywhere in the world where you have an internet connection to access the server.

6.1.2 AW Server integration modes

There are three types of integration in AW Server:

- No integration
- Full front end (or hybrid) integration (3rd party integration) with or without AW Server ***Worklist Browser***
- Seamless integration

6.1.2.1 No integration

If there is no integration, AW Server applications cannot be run from a remote system.

6.1.2.2 Full front end (or hybrid) integration (3rd party integration)

Two modes are supported depending on how the integration is used: (a) with or (b) without AW Server client ***Worklist Browser***:

a) When AW Server ***Worklist Browser*** mode is used, both the remote system and AW Server have their own patient lists. Once selecting the exam on the 3rd party system it can synchronize the selection with the AW Server client exam list.

AW Server applications can be then launched from the AW Server client.

Both the remote and AW Server database shall contain the identical patient data.

All processed data using this integration mode is stored on the AW Server database.

b) When AW Server ***Worklist Browser*** mode is not used, the application can be launched directly from the remote browser if the remote and the AW Server database contain the identical patient data.

All processed data using this integration mode is stored on the AW Server database.

6.1.2.3 Seamless integration

AW Server uses seamless integration mode with Universal Viewer.

In seamless integration mode, the 2D views in Universal Viewer desktop and 3D views of the AW Server views are synchronized to power the Advanced Applications in the Universal Viewer. Both 2D and 3D viewers are accessed and displayed via the Universal Viewer desktop. Advanced applications supported by AW Server may be launched in the Universal Viewer desktop either through inclusion in hanging protocols, or from within a viewport in the Universal Viewer desktop via a pull-down menu.

While working on 2D views in the Universal Viewer desktop and on the 3D views of the AW Server, the following functions are synchronized:

- Mouse mode
- Paging
- 3D cursor
- Zoom
- Window Width/Window level

Multiple advanced applications tools that may be familiar to users of other AW products are now accessible from the main Universal Viewer toolbar (e.g., ***2D Measure Distance***).

6.1.2.4 Starting applications

Depending on the actual integration configuration, the following options are available to start applications:

- from AW Server ***Worklist Browser*** (e.g., no integration and certain hybrid integration mode configurations),
- from the 3rd party system (PACS, Centricity PACS, CT or MR Console, etc.) (e.g., certain hybrid integration mode configurations),
- from the Universal Viewer (in seamless integration).

6.2 Downloading client

NOTE

> If the user name on the host system contains special characters the AW Server client may not be operational. If this problem is encountered, change the user login so that it does not contain special characters.

6.2.1 Downloading the client

1. In your web browser, enter the IP address of the server (e.g., http://3.70.111.10) to display the AW Server master screen.
2. Click ***Download*** at ***Client for Windows***.
3. Click ***Run*** on the ***File Download – Security Warning*** dialog box.

   Alternatively, click ***Save*** to save the installation file on your PC or click ***Cancel*** to cancel the operation.
4. If you get a ***Security Warning*** dialog box, click ***Run***.

   Alternatively, click ***Don't Run*** to cancel the operation.
5. Click ***Next*** on the ***AW Server Client Setup*** wizard to start the installation or click ***Cancel*** to stop the installation process.
6. Select a destination folder or accept the default on the ***Select Installation Folder*** dialog box and click ***Next***.

   Alternatively, click ***Back*** to return to the previous dialog or click ***Cancel*** to stop the installation process.
7. Click ***Install*** on the ***Ready to Install*** dialog box.

   Alternatively, click ***Back*** to return to the previous dialog or click ***Cancel*** to stop the installation process.
8. Click ***Finish*** on the ***AW Server Client Setup*** wizard.

6.2.2 Uninstalling and reinstalling the client

If, for any reason, you need to uninstall and reinstall the AW Server client, you first need to uninstall the client manually, then follow the instructions in the previous section to download and reinstall it.

6.3 Logging in and out of the AW Server

6.3.1 Overview

Login and logout procedures depend on the actual AW Server integration and authentication mode. The login options include, but are not limited to:

- via AW Server login screen (in no integration mode or when integrated with 3rd party DICOM hosts, see Logging in on page 34)
- via the 3rd party system (depending on the configuration, login may not be required) (in certain hybrid integration mode configurations or when integrated with 3rd party DICOM hosts)

Select the ***Keep me logged in*** check box on the AW Server login window to stay logged in the AW Server so that you will not need to log in again at the next session.

NOTE

The ***Keep me logged in*** option is only available when logging in by username and password and if enabled by a GE Field Engineer.

- via Centricity PACS (no login is required)
- in seamless integration mode no login is required.

6.3.2 Logging in

1. Start the AW Server application. This will vary by site, but some typical approaches include:
   - Clicking the shortcut on your client desktop.
   - Clicking ***Start*** from the desktop and select ***AW Server***.
2. In the AW Server login screen, enter the Server IP address, use the default address already displayed.

   If multiple IP addresses are installed, use the drop-down list to select the one you want to log in to. (see 10.2 Configuring AW Server host IP addresses at AW Server client installation on page 92).

   When logging in from an untrusted network, click the ***Show settings*** option and select the ***Secure mode*** check box.
3. Enter your username and password and click ***Login***.

   Alternatively, you can use a smartcard to log in if a smartcard reader device is installed on your computer. In this case, insert your smartcard to the device and click the ***Smartcard Login*** button.

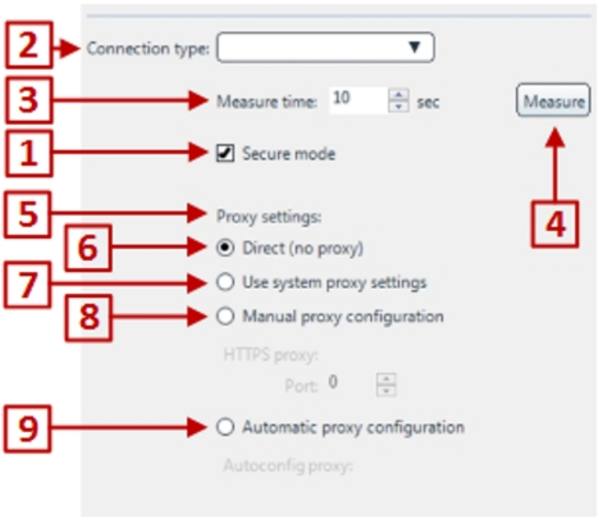
NOTE

In the event of Windows hibernation or switching users, the AW Server client session is not preserved. Logout and login are required.

6.3.3 Additional Settings

Click ***Show settings*** to expand the ***Login*** dialog screen from which you can modify the additional settings. The proxy settings are available when the ***Secure mode*** [1] check box is selected.

Figure 1 Settings



Connection type:

Measure time: 10 sec

☑ Secure mode

Proxy settings:

● Direct (no proxy)

○ Use system proxy settings

○ Manual proxy configuration

HTTPS proxy:

Port: 0

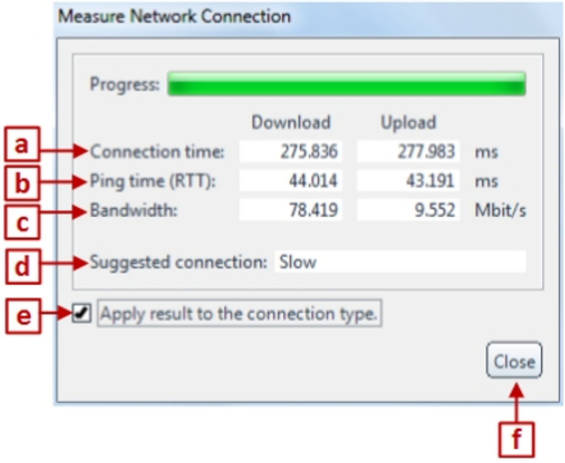
○ Automatic proxy configuration

Autoconfig proxy:

Connection type [2] describes the network performance between the AW Server and client. Automatic means that each time you log in, the client executes a network measurement and selects the connection type corresponding to the network performance to the server. If you would like to override this connection, click on the arrow and select a choice between ***Fast***, ***Medium*** or ***Slow***. The setting you choose affects different system parameters (including compression) to adapt performance to the network condition. You can later override the compression settings by selecting a different compression value displayed on the bottom of the AW Server desktop.

Measure Time [3]: Click ***Measure*** [4] to open the ***Measure Network Connection*** dialog (see Figure 2 on page 35) and run the network connectivity measurement tool.

Figure 2 Measure Network Connection dialog



Measure Network Connection

Progress:

	Download	Upload	
Connection time:	275.836	277.983	ms
Ping time (RTT):	44.014	43.191	ms
Bandwidth:	78.419	9.552	Mbit/s

Suggested connection: Slow

☑ Apply result to the connection type.

The ***Measure Network Connection*** dialog box displays the download and upload measurements for:

- ***Connection time*** [a]
- ***Ping time (RTT)*** [b]

- ***Bandwidth*** [c]

and provides a ***Suggested connection*** [d]. You can either accept this suggestion by selecting the ***Apply result to the connection type*** [e] check box, or manually set it at ***Connection type*** [2]. Click on the up and down arrows in the measure time box to set a different measurement time. The default is 10 seconds per direction (20 seconds total). Click the ***Close*** [f] button when you are finished.

Secure Mode [1] (see Figure 1 on page 35) enables a Secure Socket Layer (SSL) protocol when checked. The SSL is used to provide secure communications on the Internet. This setting might typically be used when the client is accessing the server over a untrusted network. Note that the performance is slower in secure mode.

Proxy settings [5] (see Figure 1 on page 35)

When secure mode is selected, the AWS client can make use of the HTTPS proxies to reach its server. Use these settings to set up the desired proxy.

- ***Direct (no proxy)*** [6] allows a direct connection to the AW Server

  using the intranet.

- ***Use system proxy settings*** [7] shows the proxy setting from your Operating System. On Windows systems the proxy settings are taken from those set up for Internet Explorer.
- ***Manual proxy configuration*** [8] requires a specific IP address and Port number. If this option is necessary, you must obtain this information from your IT administrator.
- ***Automatic proxy configuration*** [9] requires a URL (obtained from your IT administrator).

6.3.4 Logging out

6.3.4.1 Logout

If you click ***Logout*** in the upper right corner of the screen, you are automatically logged out of all applications currently running, any unsaved work is lost and you are returned to the login screen.

6.3.4.2 Automatic logout (only in no integration mode)

NOTICE

Your system may be configured with an automatic log out if the system has been inactive for a predetermined amount of time. The first message will notify you that the system has been inactive for a set amount of time. If you do not respond, the system automatically logs you out and your work is not saved.

6.3.4.3 Exiting a single application

To exit a single application and not log out, click on the white ***X*** on the tab. Note that in this case any unsaved work will be lost.

6.3.4.4 Clearing the clipboard when logging out

When you log out, the content that you have copied to the clipboard from the AW Server client is deleted so sensitive patient information will not be permanently available.

NOTE

In Windows 10 October 2018 and later versions, the Clipboard History feature allows you to access your copied items from every application you used. When you log out from the AW Server client, clipboard history stores your copied items from the AW Server client even after they were cleared from the clipboard. It is highly recommended not to enable the Clipboard History feature. If you need to use it, make sure to also clear clipboard history in ***Windows Settings*** > ***Clipboard*** after you logged out of the AW Server client.

6.4 Client window resolution

The proper resolution is critical to help ensure the best image quality and performance on the AW Server. If the resolution is too low, small detail information may be missed.

Use the ***Client Checker Tool*** to perform a basic test of the pixel bit depth setting of your display, the resolution of your display, etc. If these display settings do not meet the minimum requirements (e.g., if the resolution is too low, important details may not be visible), warning messages are displayed.

If you choose to ignore the warning messages, it is critical to understand that the displayed images may not be of diagnostic quality.

For detailed information about the ***Client Checker***, see Client Checker Tool.

6.5 Virtualization

AW Server is designed to be installed and run both on real (physical) computers and on virtual machines (nodes) on a host computer. Nodes on one or more host computers can be organized into cluster(s) if there is private network connection established between the nodes.

The server can be installed in a VMware vSphere® Hypervisor (ESXi 5.0, 5.1, 5.5, 6.0 or 6.5) environment.

NOTE

Using AW Server in Virtualization mode is an option, available upon request by the site.

Page intentionally left blank

Chapter 7 Client Checker Tool

7.1 Introduction

The client checker provides an initial evaluation of your operating environment by providing feedback on the quality of the client hardware, as well as the network status and basic information about your computer.

When you start the client checker, perform a basic test of your computer – the memory available, the pixel bit depth setting of your display, the resolution of your display, etc. Following this initial check, you are prompted to run the monitor quality check.

If your system fails either the initial system compatibility or monitor quality test, your system should not be used to support a medical diagnosis. Your system may require different settings or an upgrade. If that occurs, please contact your hospital or clinic support staff.

7.1.1 Monitor (display) quality check

This evaluation checks the monitor and display. It is based on the answers you give to visual cues such as how well you can visualize shades of gray, detail, etc. It does not run diagnostic tests on the hardware nor replace your normal quality assurance checks.

Every time you access this check, the access information is stored in the ***Admin/Service*** log, even if you do not execute or complete the test. After you complete the test, the results are also stored in the ***Admin/ Service*** log.

This check evaluates the monitor's ability to display:

- subtle variations in contrast
- objects without distortion
- objects with artifacts

When possible, suggestions are made on how to adjust the monitor.

7.1.2 Network summary and client information

The network summary and client information displays detailed information of interest to site IT administrators and field engineers.

7.2 Run monitor quality and client information check

1. Type in the IP address (e.g., http://3.70.111.11) of the server.

   Depending on the site configuration set by the IT department, you may also be able to enter a domain name (e.g., http://hos-client.childrenhosp.com).

2. On the AW Server master screen, click ***Launch*** next to ***Client Checker Tool***.

   If a ***Security Warning*** is displayed, select the ***I accept the risk and want to run this application*** check box at the bottom of the warning dialog, and click ***Run***.

3. The ***Client Checker Tool*** dialog opens.

4. Click ***Start*** on the ***Quality Test*** / ***Monitor Quality Check*** area, and answer the questions at steps 1 through 6 regarding grayscale, aspect ratio, resolution, and continuity by selecting the appropriate option button.

   If the check passed, a green check mark is displayed for the check that passed.

   If the check does not pass, you are given adjustment suggestions and re-prompted for an answer.

   If the check fails even after the suggested adjustments have been made, a circle crossed out in red is displayed for the check that failed.

5. At ***Step 7: Monitor Type***, select your monitor type and click ***Next***.

6. Do one of the following looking for any bad pixels (shown as white dots):

   - Click ***Check Full Screen*** to check the whole screen (recommended method).

     Click the **X** in the upper right corner of the window to close and return to the ***Quality Test*** screen.

   - Check only the currently displayed area on the right of the window.

7. Click ***Yes*** or ***No*** depending on the results of the test.

8. Click ***Next***.

9. Repeat step 6 and 7, this time looking for black dots.

10. Click ***Next*** to view the test summary.

    - If all the checks pass, you will see the following:

      ```
      Your computer and monitor has passed the image quality test. This
      does not guarantee that your system is adequate for clinical use.
      Please consult your local QA procedure.
      ```

    - If the checks do not pass, a summary of the results is displayed along with the following:

      ```
      Based on your test answers, your computer and monitor do not have
      the ability to faithfully represent an acquired image.

      WARNING! Based on responses to the preceding tests, your system
      shall not be used to support a medical diagnosis. Your system may
      require different settings or an upgrade.

      Please contact your hospital or clinic support staff.
      ```

11. To send an e-mail summary of the results, click ***Email Summary*** on the ***Summary*** area, enter the recipient's e-mail address, and send the e-mail summary.

12. You can also capture client information.

    To save client information:

    a. Click ***Client information***.

    b. Click ***Save***.

    c. Navigate to a directory or folder of your choice and enter a file name.

    d. Click ***Save*** to save the client information, or click ***Cancel*** to cancel the action.

    To send client information in e-mail:

    a. Click ***Email Configuration***.

   b. Enter the recipient's e-mail address, and send the results.

13. Click ***Close*** to close the ***Client Checker Tool*** dialog.

Page intentionally left blank

Chapter 8 Service Tools

8.1 Accessing Service Tools

Access administrator and user tools using this procedure. Note that the available tools depend on the user's permissions (i.e., **Standard** or **Administrator**).

8.1.1 From the AW Server desktop

1. Click the ***Tools*** tab on the AW Server desktop.
2. Click ***Utilities*** tab.
3. If not expanded, click ***Service Tools*** to expand the ***Service Tools*** menu.
4. Under ***Open a web browser to access administrative and service tools***, click ***Launch***.

   If your site does not have a valid certificate, a ***Security certificate warning*** is displayed. Click ***Continue to this website***.
5. Enter your ***Login*** name and ***Password*** and click ***Log in*** to view the top level service tools screen.

   If you are using a smartcard, click the ***Smartcard Login*** button.

8.1.2 From web browser

1. Type in the IP address (e.g., https://3.70.111.11) of the server.

   Depending on the site configuration set by the IT department, you may also be able to enter a domain name (e.g., https://hos-client.childrenhosp.com).
2. At the bottom of the AW Server master screen, click ***Launch*** in the ***Configuration***/***Administrative and Service Tools***.

   If your site does not have a valid certificate, a ***Security certificate warning*** is displayed. Click ***Continue to this website***.
3. Enter your ***Login*** name and ***Password*** and click ***Log in*** to view the top level service tools screen.

   If you are using a smartcard, click the ***Smartcard Login*** button.

NOTICE

The ***Security warning*** is an automatic response by web explorer program. In general, if you are not sure about the URL of the server, you would close the window. However, if you know the URL of the server (as in this case), you can confidently continue. Continuing will not make your PC vulnerable to viruses or other problems. Talk to your IT department if you have any questions or issues.

8.2 HealthPage

To access ***HealthPage***:

1. Access Service Tools (see Accessing Service Tools).
2. Click ***HealthPage***.

HealthPage provides the following information:

- ***Hardware Subsystem*** status

  Each time you start the service and administrator tools, a system summary is displayed. The status is color coded to give you a quick visual report.

  - Green: OK
  - Red: a problem may exist that should be addressed before continuing

  If there are failures, detailed information is stored in the Log Viewer which is only accessible by Service personnel.

  Click ***Sensor Details*** to get sensor information. Sensor details will typically be used by the field engineer for in depth information on the server sensors.

  Click ***Refresh*** to update the status information.

  Note that, if applicable, ***Virtual Machine*** status is also displayed.

- ***System Configuration***

  Click ***Refresh*** to update the status information.

- ***Version Information***

  Click ***Refresh*** to update the status information.

- ***Configuration and status***

  - Click ***Pull from system*** to obtain and save configuration and status information on your client machine.
  - Click ***Display*** to display configuration and status information in Service Tools.

    The information will be shown in a new window. Click ***Hide*** to close the window.

- ***Software Subsystem***

  You can restart all the software subsystems by clicking ***Restart*** in the ***Software Subsystem*** area of the screen. Restarting these services will disconnect users immediately without warning and cause any unsaved work to be lost.

  NOTE

  > Restart does not affect ***Firewall (pnf)*** and ***Time Server (ntpd)***, these will not be restarted.

- ***Software Subsystem essential for Service Tools***

Click ***Refresh All*** to update all status information.

8.3 Initial Configuration

8.3.1 Overview

Initial Configuration in Service Tools provides the following tools:

- ***Contact***

  Use ***Contact*** to manage configured contacts.

- ***Time Settings***

  Use ***Time Settings*** to manage date and time settings, configure Network Time Protocol Server.

- ***Database Deletion Settings***

  Use ***Database Deletion Settings*** to set image auto deletion policy and enable/disable the manual delete option for the ***Worklist Browser***.

- ***SNMP Configuration***

  Use ***SNMP Configuration*** to manage Simple Network Management Protocol (SNMP) configuration.

- ***Scalability***

  Use ***Scalability*** to manage and display scalability settings.

- ***Audit Trail (EAT)***

  Use ***Audit Trail (EAT)*** to view audited events.

8.3.2 Managing contacts

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Initial Configuration***.
3. Click ***Contact***.

   The ***Set up contact info*** screen opens.
4. Manage contact data:
   - To add a contact, click ***Add*** and enter in relevant data. ***Type*** and ***Name*** must be entered. All other fields are optional.
   - To edit a contact, click on an entry in the ***Configured contacts*** field. The form is populated with the current information. Make changes or additions, and then click ***Apply*** to save this data or click ***Cancel*** to discard the changes.

     Note that you cannot edit the ***Type*** value of the default contacts (i.e., ***Hospital IT***, ***GE Contact*** and ***Hospital admin***).
   - To delete a contact, click on an entry you want to delete in the ***Configured contacts*** field, and click ***Delete***.

     Note that you cannot delete the default contacts (i.e., ***Hospital IT***, ***GE Contact*** and ***Hospital admin***).

8.3.3 Time Settings

8.3.3.1 Accessing the time settings screen

To access the time settings screen:

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Initial Configuration***.
3. Click ***Time Settings***.

   Perform date and time settings, configure Network Time Protocol Server screen opens, showing the ***Date/Time*** and ***Time Server*** tabs. It also displays ***Daylight Saving Time Clock Changes*** information.

8.3.3.2 Setting date and time

Click the ***Date/Time*** tab on the ***Perform date and time settings, configure Network Time Protocol Server*** screen.

To set the region and the time zone:

1. Click the arrow under ***Region*** and select the region.
2. Click the arrow under ***Timezone*** and select the corresponding time zone.
3. Click ***Apply*** to save the settings or click ***Cancel*** to discard the changes.

To set date and time:

1. In the ***Date*** text field, type in the date in the required format as shown in the example next to the text field (i.e., *(M)M/(D)D/YYYY*).
2. In the ***Time*** text field, type in the time in the required format as shown in the example next to the text field (i.e., *(H)H/(M)M/(S)S*). Use 24 hour time format.
3. Click ***Apply*** to save the settings or click ***Cancel*** to discard the changes.

8.3.3.3 Configuring time server

If your site uses a Network Time Protocol (NTP) server, use this tool to synchronize the AW Server time with that of the network time server.

Click the ***Time Server*** tab on the ***Perform date and time settings, configure Network Time Protocol Server*** screen.

To add a network time server:

1. At ***Configure NTP Client***/***Server address***, enter the network time server IP address.
2. Click ***Check address*** to verify the network (TCP/IP) connection.
3. Click ***Add*** if you want to add the server address to the list of configured NTP servers.

To delete a configured network time server:

1. Click on the entry you want to remove in the ***List of configured NTP servers*** field.
2. Click ***Remove*** to delete the selected network time server.

At ***Manage NTP client***/***Status***, the current status of the network time server is displayed.

You can start/restart or stop the NTP client by using the ***Start/Restart*** or ***Stop*** buttons, respectively, at the bottom of the screen. Click ***Refresh*** to update the status information.

If the server cannot be reached, the NTP synchronization will continue without posting a failure notification.

8.3.4 Setting the auto and manual delete functions

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Initial configuration***.
3. Click ***Database Deletion Settings***.

   The ***Database Deletion Settings*** screen opens, which allows you to set the image auto delete policy and enable/disable the manual delete option for the ***Worklist Browser***.

   NOTICE

   Enabling the auto delete function may result in possible loss of data.

   - To set the image auto delete policy:

     a. On the upper ***Auto Delete Settings*** area, click the ***On***/***Off*** option button at ***Auto delete status*** to turn the auto delete function on/off, respectively. The function is turned off by default (the ***Off*** option button is selected).

        The value on the right of ***Current % of image data base utilized by system*** shows the extent of actual image database system utilization in percentage.

        When image auto deletion is turned off, the settings are greyed out, they cannot be modified.

        When image auto deletion is turned on, set the auto delete settings as follows:

        - At ***Start when image database reaches***, enter the value of image database utilization in percentage at which, when reached, the image auto deletion will start.
        - At ***Stop when image database reaches***, enter the value of image database utilization in percentage at which, when reached, the image auto deletion will stop.
        - At ***Remove image(s) from system database older than***, enter the number of ***months***, ***days*** and ***hours*** the images older than have to be deleted.
        - In the ***Auto Delete Scheduling Mode*** section, you can choose between two different options:
        - At ***Start auto delete of image(s) daily at***, enter the image auto deletion start time using the 12–hour clock time convention in the format **<hour>:<minute> <AM/PM>** (hour:minute values and AM/PM separated by one space); for example, **7:30 PM** (half past seven in the evening).
        - or

  - At ***Start auto delete process every***, enter the amount of time in hours how frequently you want the image auto deletion to start; for example, enter **8** to start the image auto deletion every 8 hours.

  b. Click ***Apply*** to save the settings or click ***Cancel*** to keep the original settings and discard the changes.

- To enable/disable manual deletion in the ***Worklist Browser***:

  a. On the lower ***Delete option for worklist browser*** area, click the ***On***/***Off*** option button at ***Delete option status*** to turn the manual delete function on/off, respectively.

  The function is turned off by default (the ***Off*** option button is selected).

  b. Click ***Apply*** to save the settings or click ***Cancel*** to keep the original settings.

8.3.5 Configuring Simple Network Management Protocol settings

Simple Network Management Protocol (SNMP) configuration observes the connection between the AW Server and a hardware and software monitoring server. Any AW Server failures will cause a message to be sent to the configured SNMP server. This application works in the background and has no effect on available resources. Use the procedure below to add, change or verify a setting.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Initial Configuration***.
3. Click ***SNMP Configuration***.

   The ***Configure Simple Network Management Protocol settings*** screen opens.
4. At ***SNMP trap configuration***, select ***Enabled*** to activate or ***Disabled*** to deactivate the monitoring.
5. Enter in the IP address of the monitoring server in the ***Monitoring server IP address*** text field.
6. Click ***Check IP*** to verify the TCP/IP connection.
7. Click ***Apply*** to save the address or click ***Cancel*** to discard the changes.

8.3.6 Displaying scalability settings

AW Server offers the scalability feature to optimize the number of applications that can be used simultaneously.

Resource distribution to a new user does not depend on the number of already logged-in users with active sessions, but on the number of available slices to load. For example, if a new user is logged in the server and starts an application, this user can start working regardless of the number of active users as long as the exams/series the user is attempting to load have an amount of slices that is within the available loadable slice number.

If the exam/series slice number exceeds the available slice number, the user will not be able to start the session.

NOTE

Scalability is available only in AW Servers running on virtual machines and integrated with a PACS remote host system. A prerequisite for using the scalability feature is that all virtual computers it is used on have exactly the same hardware configuration (hard disk, processor, etc.).

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Initial configuration***.
3. Click ***Scalability***.
4. The table in the ***Manage and display scalability settings*** screen provides the following information:
   - ***NODE [IP ADDRESS]***: in cluster mode, it lists the host name and IP address of each node in the cluster. Note that the host name is also the link to the Service Tools page of the node.

     Node status symbols are as follows:

     - ✓ : node is active (broadcast information received),
     - ⚙⚠ : there is a problem with the preference servers,
     - 🛠 : node is in Maintenance Mode,
     - ⚠ : node has certain problems,
     - ❌ : node is inactive (no broadcast information received).
   - ***CLIENTS***: displays the number of clients connected to each node.
   - ***APPLICATIONS***: displays the number of applications running on each node.
   - ***SLICES***: displays the number of slices for each node (used/total).
   - ***CPU***: displays the CPU usage of the node.
   - ***MEMORY***: displays the memory usage of each node.
   - ***DISK***: displays the disk partition usage of each node.
   - ***VERSION***: displays the version information and selected integration mode compatibility status between the platform/installed applications and the cluster golden set.
     - if the status is `OK`, the version information and selected integration mode of the platform/installed applications are the same as those of the cluster golden set,
     - if the status is `Mismatch`, there is a mismatch between the version information and selected integration mode of the platform/installed applications and those of the cluster golden set.
     - Click on the status to open the ***Version information/Golden set*** dialog that displays detailed version information.

       If the status is `OK`, click ***Hide*** to close the ***Version information/Golden set*** dialog.

       If the status is `Mismatch`, you can either click ***Set as golden set*** to save the current set as golden set or click ***Hide*** to close the ***Version information/Golden set*** dialog.

- ***LICENSE SERVER***: lists the IP address(es) of the configured license server(s).

  The symbols before the IP addresses have the following meanings:

  - ✓ : the license server is running and the IP addresses in the cluster are the same,
  - ⚠ : the IP address of the license server does not match the cluster,
  - ❌ : the license server is unavailable.

5. Click ***Refresh*** to update the scalability settings information.

8.3.7 Viewing audit events

The Administrator can view the content of specific audit events stored in the local repository.

NOTE

> If specific search activities are needed, the hospital is advised to implement these activities on a remote syslog server set up for this purpose.

NOTE

> The Administrator is advised not to modify the configuration that has been set up and to request help from GEHC Service for the configuration.

8.3.7.1 Accessing the audit events screen

1. Access Service Tools (see 8.1 Accessing Service Tools on page 43).
2. Click ***Initial Configuration***.
3. Click ***Audit Trail (EAT)***.

   The ***Perform Enterprose Audit Trail configuration*** screen opens.

8.3.7.2 Viewing audit events

1. Click the ***Local Repository*** tab to access the list of audit events.
2. Select the ***On*** or ***Off*** radio buttons to turn the local repository on or off.
3. Audit events are listed on the left side in a chronological order displaying event ID, time of the event and outcome.

   Use the arrows on the top or the bottom of the list to turn pages.

   Optionally, click ***Refresh*** to update the list of audit events.
4. Click any event in the list to view the details. The details of the event will be displayed on the right side.

   You can also view the event details in an unformatted XML format by clicking the ***Display Raw XML*** button.

8.4 Administrative

8.4.1 Configuration

8.4.1.1 Configuring and managing DICOM Hosts

Before adding a host, you must know the hospital name to be printed on the film, the Label (printer name), Host name, AET (Application Entity Title), IP address and host port. If this information is not known, it can be obtained from the site administrator or IT department.

8.4.1.1.1 Access the DICOM host (network) configuration page

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***DICOM Hosts***.

   The ***Perform DICOM hosts configuration*** screen opens.

8.4.1.1.2 Add a new host

1. In the ***Perform DICOM hosts configuration*** screen, click ***Add new*** and enter the following:
   - ***Name*** (to be used on the Host icon in the user interface)
   - ***Host name***
   - ***Application Entity Title*** (for DICOM hosts)
   - ***IP address*** of the remote Host

     Click ***Check IP*** to verify the network (TCP/IP) connection between the AW Server and host.
   - ***Port*** number (for DICOM hosts)

     Click ***Check DICOM*** to verify the connection between the AW Server and DICOM port.
   - Select the ***Query/retrieve supported*** and/or ***Custom Search*** check boxes if applicable for DICOM hosts.
   - Select the ***Institution*** and/or ***Reading Physician*** checkboxes to request these DICOM tags to be retrieved.
   - Select the ***Storage Commitment Supported*** check box if capability (for DICOM hosts) is supported.

     if you selected ***Storage Commitment Supported***, enter the following information:
     - ***SC Host name***
     - ***SC AE title***
     - ***SC IP address***

       Click ***Check IP*** to verify the network (TCP/IP) connection.

    - ***SC Port***

      Click ***Check DICOM*** to verify the connection.

  - Click the ***Allow Query***, ***Allow Retrieve*** and/or ***Allow Store*** check boxes if applicable.
  - Enter any comments.
  - Optionally, enter the ***Authentication URL*** of the web services of the remote host.

2. Additional settings are available for integration with 3rd party DICOM hosts only:
   - ***Preferred compression format***
   - ***Allow speed-up of C-FIND query***
   - ***Allow early response for C-STORE***
3. Click ***Apply*** to save or ***Cancel*** to discard the changes.
4. Click ***Refresh*** to see the latest additions/changes.

8.4.1.1.3 Modify an existing host

1. In the ***Perform DICOM hosts configuration*** screen, click on an entry in the ***Current configured hosts*** box to view information associated with that host.
2. Type over existing information, or enter new information in a blank field and click ***Apply***.
3. Click ***Refresh*** to see the latest additions/changes.

8.4.1.1.4 Delete an exisiting host

1. In the ***Perform DICOM hosts configuration*** screen, click on an entry in the ***Current configured hosts*** box to view information associated with that host.
2. Click ***Delete*** and ***OK*** in the confirmation dialog box.

8.4.1.2 Configuring and managing DICOM printers

Before adding a printer, you must know the ***Printer Label***, ***Host name***, ***Application Entity Title (AET)***, ***IP address*** and printer port. If this information is not known, it can be obtained from the site administrator or IT department.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***DICOM Printers***.

   The ***Perform DICOM printers configuration*** screen opens.

8.4.1.2.1 Add a new printer

1. In the ***Perform DICOM printers configuration*** screen, enter hospital name (the name to be printed on the film) in the ***Hospital name for Filmer*** field.

2. Click ***Apply***.
3. Click ***Add*** and enter the following:
   - ***Label*** - this is a name of your choice.
   - ***Host name***
   - ***Application Entity Title***
   - Network ***IP address*** of the printer.

     Click ***Check IP*** to verify the network (TCP/IP) connection between the AW Server and printer.
   - ***Port*** number.

     Click ***Check DICOM*** to verify the communication between the AW Server and printer.
4. Select ***Layouts*** as required.
5. Select and enter ***Film size*** parameters and remaining DICOM Printer parameters as defined by the vendor's printer DICOM conformance statement (***Filming mode***, ***Printer pixel size***, ***Density***, ***Magnification type***, ***Smoothing factor***, ***Trim***, ***12 bits image supported***, ***Color supported***, ***Memory***, and ***Configuration information***).
6. Enter any comments and click ***Apply*** to save or ***Cancel*** to discard the changes.
7. Click ***Refresh*** to see the latest additions/changes.

8.4.1.2.2 Modify or delete an existing printer

1. In the ***Perform DICOM printers configuration*** screen. click the entry you want to modify in the ***Current configured DICOM printers*** field to view information associated with that printer.
2. To modify, enter new information and click ***Apply***.
3. To delete, click ***Delete*** and ***OK*** in the confirmation dialog box.
4. Click ***Refresh*** to see the latest additions/changes.

8.4.1.2.3 View recently added printers

If a printer was added remotely and you do not see it, click ***Refresh***.

8.4.1.3 Configuring and managing PostScript printers

Before adding a printer, you must know the Printer name, IP address and printer port. If this information is not known, it can be obtained from the site administrator or IT department.

1. Access Service Tools (see 8.1 Accessing Service Tools on page 43).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***PostScript printers***.

   The ***Perform PostScript printers configuration*** screen opens.

8.4.1.3.1 Add a new printer

1. Click ***Add*** and enter the following:
   - ***Name*** - this is a name of your choice
   - ***Address[:Port]*** - network IP address of the printer

     Entering a port is not mandatory. If not specified otherwise, port 9100 is used by default.
   - ***Paper size***
2. Click ***Apply*** to save or ***Cancel*** to discard the changes.
3. Click ***Refresh*** to see the latest additions/changes.

8.4.1.3.2 Modify or delete an exisiting printer

1. In the ***Perform PostScript printers configuration*** screen, click the entry you want to modify in the ***PostScript printers*** field to view information associated with that printer.
2. To modify, enter new information and click ***Apply***.
3. To delete, click ***Delete*** and ***OK*** in the confirmation dialog box.
4. Click ***Refresh*** to see the latest additions/changes.

8.4.1.3.3 View recently added printers

If a printer was added remotely and you do not see it, click ***Refresh***.

8.4.1.4 Authorizing and authenticating users

8.4.1.4.1 Overview

Enterprise users must use the group names established on the enterprise server. Each group can have an unlimited number of members.

Use the EA3 tool to manage the access given to users on the server. Each user must be assigned to a group and each group must be assigned a role which determines the access level. For example in the table below:

- One member (Mary) belongs to the FE group, has service level privileges and can access service, administrator and standard user tools.
- One member (Jessie) belongs to the IT group, has administrator privileges and can access administrator and standard tools. The lead tech (in some instances such as in a stand-alone site) might belong to this group.
- Three members (Ella, Samantha and Lamar) belong to the Technologist group, have standard privileges and can access only standard user tools.
- Two members (Ralph and Joe) belong to the Radiologist group, have standard privileges and can access only standard user tools. Note that the radiologist and technologist group have the same privileges and could be combined into one group if desired. You can have any number of groups with the same access level.

- Four members (Andrea, Kate, Bill and David) belong to the Referring Physicians group, have limited privileges and can only access Reformat. In addition, to view patient data they must know the patient's first and last name and either the date of birth or the patient ID.

User/Member	Group	Access Level	Definition
Mary Marche	Field Engineer (FE)	Service	Access to all tools.
Jessie Johnson	IT	Administrator	Access to all features and tools with the exception of service tools.
Ella Enrich Samantha Smith Lamar Lopez	Technologist	Standard	General access for most users. Can see database and access user tools, but not administrator or service tools.
Ralph Rogers Joe Johnson	Radiologist	Standard	General access for most users. Can see database and access user tools, but not administrator or service tools.
Andrea Anderson Kate Kruthers Bill Burton David Davidson	Referring Physician	Limited	Most restricted access for casual user. Cannot access any user tools or see the full database. Must know the patient's last name and Patient ID to view exam data.

NOTE

> If your site has an active directory/LDAP server (for example, user ID, billing, email, intra-, internet access, etc.), you must configure the server connection via the ***Enterprise*** tab. In addition, you must make sure the group from the active directory/LDPA server is mapped to an enterprise group.

8.4.1.4.2 Managing local users

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Users (EA3)***.

   The ***Perform Enterprise Authentication, Authorization and Audit configuration*** screen opens.
5. Click the ***Local Users*** tab.

8.4.1.4.2.1 Add a new user

1. At the top right of the ***Local Users*** tab, click ***Add Local User***.

   The ***Add User*** dialog box opens.
2. Enter the following data for the new local user:
   - ***User ID***
   - ***Full Name***

- ***Password***
- ***Confirm Password***

3. Click ***Add User*** to add the new local user to the system or click ***Cancel*** to discard changes and close the dialog.

8.4.1.4.2.2 Assign a user to group(s)

1. In the ***Local Users*** tab, click on the user you want to add to user group(s) in the ***Local Users*** list.
2. Click ***Add To Groups***.

   The ***Add Membership For User (<user name>)*** dialog box opens.
3. In the ***Add Membership For User (<user name>)*** dialog box, select the group(s) in the ***Choose groups to add user as a member*** list you want to add the user to. All groups except those that the user is already a member of are displayed. Hold down the ***Ctrl*** key to select multiple groups.
4. Click ***Add Membership*** to add the user to the selected group(s) or click ***Cancel*** to discard the changes and close the dialog.

8.4.1.4.2.3 Remove a user from group(s)

1. In the ***Local Users*** tab, click on the user you want to remove from user group(s) in the ***Local Users*** list.
2. Click ***Remove From Groups***.

   The ***Remove Membership (<user name>)*** dialog box opens.
3. In the ***Remove Membership (<user name>)*** dialog box, select the group(s) in the ***Choose groups to remove user as a member*** list you want to remove the user from. All groups the user is a member of are displayed. Hold down the ***Ctrl*** key to select multiple groups.
4. Click ***Remove Membership*** to remove the user to the selected group(s) or click ***Cancel*** to discard the changes and close the dialog.

8.4.1.4.2.4 Configure password settings for all local users

NOTICE

Do not use special characters in the password.

1. At the top of the ***Local Users*** tab:
   - ***Max Logon Attempts Before Lock***: enter the number of attempts users are allowed before they are locked out of the system,
   - ***Minimum Password Length***: the minimum length of a password (number of characters),
   - ***Lock Duration (Minutes)***: how long they are locked out if they exceed the maximum number of log in attempts.
2. Click ***Apply Configuration***.

   Restore Configuration resets the values since you last clicked ***Apply Configuration***.

8.4.1.4.2.5 Configure password settings for individual users

1. At the bottom of the ***Local Users*** tab, select the ***Locked*** check box if you want to stop the user from logging in without removing them from the system.
2. Click ***Apply Configuration***.

   Restore Configuration resets the values since you last clicked ***Apply Configuration***.

8.4.1.4.2.6 Remove user, change password or name

Select a user name from the local users area.

In the middle of the ***Local Users*** tab, click ***Change Name***, ***Change Password***, or ***Remove User*** and make changes as necessary.

8.4.1.4.3 Managing groups

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Users (EA3)***.

   The ***Perform Enterprise Authentication, Authorization and Audit configuration*** screen opens.
5. Click the ***Groups*** tab.

8.4.1.4.3.1 Create a group

In the ***Groups*** tab:

- Click ***Add Local Group*** to add a new local user group.

  The ***Add Local Group*** dialog box opens.

  1. In the ***Add Local Group*** dialog, enter ***Group Name***.
  2. Click ***Add Group*** to add the new local user group to the system or click ***Cancel*** to discard the changes and close the dialog.
- Click ***Add Enterprise Group*** to add a new enterprise user group.

  The ***Add Enterprise Group*** dialog box opens.

  1. In the ***Add Enterprise Group*** dialog, enter ***Group Name***.
  2. Click ***Add Group*** to add the new enterprise user group to the system or click ***Cancel*** to discard the changes and close the dialog.

Depending on whether you have created a new local or enterprise group, the new user group shows up in the ***Local Groups*** or in the ***Enterprise Groups*** list, respectively.

8.4.1.4.3.2 Assign roles to a group

1. In the ***Groups*** tab, click on a group in the ***Local Groups***/***Enterprise Groups*** list.

   Any users already assigned to the group are displayed in the ***Group Members*** list.

2. In the ***Roles*** pane, select the box(es) next to a role(s) you want to assign to the group.

   The roles you assign to groups determine the group privileges.

   NOTE

   > Service privileges are required to assign ***GE Service*** role to a group.

3. Click ***Apply Roles***.

8.4.1.4.3.3 Remove a group

1. In the ***Groups*** tab, click on the group you want to delete in the ***Local Groups***/***Enterprise Groups*** list.
2. In the ***Group Name*** pane, click ***Remove Group***.

   The ***Confirm Removal (<group name>)*** dialog box opens.

3. Click ***Confirm Removal*** to delete the group or click ***Cancel*** to keep the group and close the dialog.

8.4.1.4.4 Setting up Enterprise users

NOTICE

> You can set up the AW Server to use the log in credentials of the enterprise authentication. This procedure has to be performed by personnel familiar with Enterprise systems.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Users (EA3)***.

   The ***Perform Enterprise Authentication, Authorization and Audit configuration*** screen opens.

5. Click the ***Enterprise*** tab.

8.4.1.4.4.1 First steps

1. At the top of the screen, select the check boxes next to:
   - ***Enable Enterprise Authentication*** to allow users to log on with enterprise credential.
   - ***Cache Enterprise Users*** to allow users to log onto an enterprise system without a connection to the directory server.
   - Enter in a value for the ***Enterprise Authentication Latency (Seconds)***.

     If there is no response from the enterprise server within this time, the login will fail.

2. Click ***Apply Configuration*** to save or click ***Restore Configuration*** to discard the changes.

8.4.1.4.4.2 Configure the AW Server with the Enterprise system

1. In the ***Configuration Instructions*** pane:
    a. Click ***Auto-detect Server Name***.

       The configuration information is automatically filled in on the right hand pane below ***Server Configuration***.

       If auto-detection does not work, type in the server name and IP address.

    b. Click ***Test Connection***.

    c. Click ***Generate Defaults***.

    d. Click ***Apply Configurations***.

       The LDAP configuration information is automatically filled in on the right hand pane below ***LDAP Configuration***.

    e. Enter the ***Username*** and ***Password*** of the user as it exists on the enterprise server and click ***Login***.

       Verify the results in the ***Login Results*** box. The group to which the user belongs is of particular importance. You will use this information when you create a group.
2. Click ***Apply Configuration*** at the bottom of the right hand pane if the configuration is correct or click ***Restore Configuration*** to discard changes.

8.4.1.5 Configuring Smartcard authentication

8.4.1.5.1 Access the Smartcard authentication configuration screen

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Smart Card Configuration***.

   The ***Smart card login configuration*** screen opens.

8.4.1.5.2 Configure Smartcard authentication

1. Select the ***Enable Smart Card Login*** check box to allow users to log in using a smartcard.
2. In ***Active Directory Configuration***, enter the following information to configure the server and define user mapping attributes:
    - ***Server Configuration***:
        - ***Use SSL***: select this check box to use SSL network protocol
        - ***Server name / IP***
        - ***Port*** (optional)
        - ***User***: can be set using LDAP DN, domain format or pre-Windows 2000 format
        - ***Password***

    - ***DN***

  - ***User Mapping***:
    - ***Login name attribute***
    - ***First name attribute***
    - ***Last name attribute***
    - ***Group attribute***
    - ***UPN attribute***

3. In ***JSON Web Token (JWT) Settings***, click the ***Generate*** button to generate a random JWT secret.
4. In ***Proxy settings***, select ***Direct (No Proxy)*** if no proxy server is used, or select ***Manual Proxy Configuration*** to manually add the address of the proxy server.
5. In ***Trusted Certificate Authorities (CAs)***:
   - Click the ***Choose Files*** button to navigate to the location of the certificate you want to add, then click ***Send to system*** to upload the certificate to the system.
   - To remove a certificate, select the check box next to the certificate you want to remove and click the ***Remove Selected Certificates*** button.
6. Click ***Apply Configuration*** to save and apply the changes you made.

   Restore Configuration resets all the changes and restores the default configuration.

8.4.1.6 Setting Client Timeout

You can set up an automatic messaging system to manage inactive clients. The first message is sent requesting a response from the client. If a response is not received in a specific amount of time, the client is automatically logged out. The time before the first message is displayed and the subsequent forced logout is set by you. This feature is turned off by default.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Client Timeout***.

   The ***Client timeout settings*** screen opens.
5. Click ***Enable Inactivity Timeout***.
6. At ***Minutes to wait before displaying message***, enter a value for the amount of time a user must be inactive before a message is displayed on their client.
7. At ***Minutes to wait before automatically logging out the user***, enter a value for the amount of time the system will wait for an acknowledgement from the user before automatically logging them out.
8. Click ***Apply***.

NOTICE

Enabling this feature could cause users to lose their work if they do not respond to the system messages.

8.4.1.7 Configuring Preprocessing

If your site has a Preprocessing license configured, and you have set up the appropriate parameters, preprocessing can execute without user interaction. When an exam is sent to the AW Server, the series descriptor is searched, looking for a match set on the ***Preprocessing*** screen. If a match is found, and there are enough available resources, the corresponding application will start automatically in the background and save the results in a save state series. For example, if you enter CTA Head in the descriptor field for Head-Autobone Xpress, the Autobone XPress application will start without user intervention and save the results in a save state series.

NOTE

When AW Server is integrated with a 3rd party DICOM host, the 3rd party host can trigger Preprocessing on the AW Server by sending a DICOM Instance Availability Notification (IAN) message for newly available series. To enable this feature, the remote DICOM host(s) must be configured to send IAN messages to the dedicated AEtitle of the AW Server named "AEtitle**_ds**", port 4010.

NOTE

If your site does not have a preprocessing license, the preprocessing screen displays the `"Preprocessing application is not available"` message.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***Preprocessing***.

   The ***Preprocessing configuration*** screen opens.
5. Select the check box to enable the corresponding Preprocessing application.
6. Enter a series descriptor that the AW Server will use to search.

   If a received series contains the words entered in the series descriptor box, processing on that series will automatically begin and the results will be saved in an Auto Save State series.

8.4.1.8 Configuring MailSender

The MailSender service allows applications using the email sending service to send email reports to predefined contacts/recipients.

NOTE

Entering the MailSender license is a pre-requisite to configuration. Please contact your GE Service Representative for assistance.

8.4.1.8.1 Accessing MailSender Configuration

1. Access Service Tools (see 8.1 Accessing Service Tools on page 43).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***MailSender***.

   The ***MailSender Configuration*** screen appears.

8.4.1.8.2 Configuring MailSender

1. Below ***Enable MailSender?***, select ***Yes*** to enable the mail sending service, or select ***No*** to disable it.
2. Complete the mail sender address by entering the domain in the ***Sender Address*** field.

   This is the email address of the sender of the email. It contains the name of the application and the name of the host corresponding to the application/host from which the report will be sent. You will not be able to reply to this address.
3. Configure the local SMTP mail server:
   - Enter the IP address or the fully qualified domain name of the mail server in the ***SMTP Server Address*** field.
   - Enter the mail server port number in the ***SMTP Server Port*** field.

     Port **587** for TLS protocol, or port **25** in case of an unsecured connection.
   - Select the protocol in the ***SMTP Security Level*** field.

     NOTE

     By default, **TLS** protocol is selected. It is highly recommended to keep to default SMTP security level. By selecting **NO**, you configure the mail server to use an unsecured connection that does not require a CA certificate.
4. Upload the ***SMTP Server CA Certificate***:
   - Click the ***Choose File*** button to navigate to the location of the certificate you want to add, then click the ***Upload*** button to send the certificate to the system.

     NOTE

     Only CA certificates in PEM (Privacy-Enhanced Mail) format can be uploaded to the system.

     The expiration date of the CA certificate in use is displayed on the screen. If the certificate has expired, the expiration date is displayed in red.
   - To change the CA certificate in use, click the ***Remove*** button first, then navigate to the location of the certificate you want to upload using the ***Choose File*** button and click ***Upload*** to send the new certificate to the system.
   - Enter a ***Notification Address***.

     A notification email will be sent weekly if the certificate expires in less than 90 days.

A warning message is also displayed on the top of all Service Tools pages depending on the status of the certificate in use.

Click the displayed message to open the MailSender configuration page.

5. At ***Test Mail Sending***, click the ***Test Connection*** button to check if the configured SMTP server accepts SMTP connection with the selected settings.

   If the connection is successful, the ***Success*** label highlighted in green is displayed.

   If the connection is unsuccessful, the ***Fail*** label highlighted in red is displayed.
6. Click ***Apply*** to save or ***Cancel*** to discard the changes.

   Once you apply the changes, the system returns feedback on the success of the configuration.

8.4.1.8.3 Configuring the email distribution list

The email distribution list must be configured for each application using the email sending service.

See section 8.3.2 Managing contacts on page 45 for the procedure of adding, editing or removing recipients.

For further details, please refer to the user documentation of the corresponding application.

8.4.1.9 Managing End Of Review

If you have a DICOM host configured on your AW Server, and End of Review is set up, you can have processed images automatically networked to a DICOM host. Upon exiting a processing application, a ***Yes*** response to the ***End Of Review*** prompt forwards the processed series to any DICOM host configured on the server.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Configuration***.
4. Click ***End Of Review***.

   The ***Manage End Of Review*** screen opens.
5. Select the check box in the ***Status*** column in front of the ***Host name*** to make the item active.
6. Under ***Type***, use the drop-down menu to choose which series (***generated*** or ***all***) can be automatically sent to a networked host.
7. Click the button below ***Modality*** to view choices.
8. Select the ***Select All*** check box to select all modalities or select individual modalities.
9. Click ***Apply*** to save or ***Cancel*** to discard the changes.

8.4.2 Utilities

8.4.2.1 Clients

8.4.2.1.1 Broadcasting messages to clients

Via the ***Broadcast message*** tab in the ***Manage clients*** screen, you can display a message to all current clients and future users when they log in. Whenever possible, a message should be broadcast to all users currently logged on before you disconnect clients.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Clients***.

   The ***Manage clients*** screen opens.
5. Click the ***Broadcast message*** tab.
6. On the ***Broadcast message*** tab, choose a message from the ***Broadcast message templates*** drop-down list, or place cursor in the ***Broadcast message*** text box and type the appropriate message (e.g., `System will be shut down at 2300 hours`).
7. Click ***Set message***.

   This message will be immediately displayed to all clients currently logged on and anytime a new user logs in.

   - To delete the message from the server, click ***Clear message***.
   - To view the latest message set on the server, click ***Query message***.
   - To set a message that all users will see when they log in, click ***Set message***.

8.4.2.1.2 Disconnecting clients

Disconnecting clients can be done in or out of maintenance mode. When disconnecting clients, any unsaved work will be lost. Whenever possible, give users a chance to save their work and log off using the broadcast message procedure.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Clients***.

   The ***Manage clients*** screen opens.
5. Click the ***Manage clients*** tab.
6. Click ***Refresh*** to see the most recent list of users logged on.

If client data cannot be retrieved (due to a temporary network disconnect for example), the logged in client section will display a row filled in with the word `"unknown"`. Try to get the actual client information by clicking ***Refresh***.

7. Select the check box in the title bar to log off all clients or the check box in front of one or more specific clients.
8. Click ***Disconnect Selected***.

   A warning message is posted indicating that any work not saved by users will be lost and asks if you wish to continue.
9. Click ***OK*** to immediately send the disconnect message and disconnect selected clients or ***Cancel*** to return to the page without terminating clients.

8.4.2.2 Viewing and modifying network queue

NOTE

Any user can view the network queue, but modifying entries requires administrator or service privileges.

Any exams scheduled, but not yet sent to another system on the network, are placed in a network queue. As soon as the current exam is completely transferred, the next exam is automatically networked. You can view or modify the jobs in the network queue.

8.4.2.2.1 View a network queue

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Network Queue***.

   The ***Manage DICOM network queue*** screen opens.
5. Click ***Refresh*** to see the latest status.

   The following information is displayed:

   - ***E/S/I***
   - ***Type***
   - ***Status***
   - ***Progress***
   - ***Date***
   - ***Source***
   - ***Target***

To view network queue history:

1. On the ***Manage DICOM network queue*** screen, click ***Show history***.
2. Click ***Refresh*** to refresh network queue history.

8.4.2.2.2 Modify network queue entries

1. Select on one or more check boxes on the left of the queue entry.
2. Click ***Pause***, ***Resume***, ***Retry*** or ***Cancel*** to perform the corresponding action. The action will be applied to all entries selected.
3. Click ***Refresh*** to see the updated queue.

8.4.2.3 Managing DICOM print queue

Any print jobs sent to a printer but not yet printed, are placed in the print queue. When the current print job finishes, the next print job in line is automatically printed. You can view or modify the jobs in the print queue.

8.4.2.3.1 View a print queue

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Print Queue***.

   The ***Manage DICOM Print queue*** screen opens.
5. Click ***Refresh*** to display the latest printing status.

8.4.2.3.2 Modify print queue entries

1. Select on one or more check boxes at the left of the queue entry.
2. Click ***Cancel Job*** to remove the job from the queue.

   Pause Queue and ***Resume Queue*** are applied to the entire queue, not just selected entries.
3. Click ***Refresh*** to see the updated queue.

8.4.2.3.3 Queue history

- Click ***Show history***.
- Click ***Refresh*** to see the latest entries.
- Click ***Clear History*** to delete all the entries.

8.4.2.4 Image Database

8.4.2.4.1 Managing database

Within the manage database screen, you can get detailed information about exams, series or images as well as download or delete specific exams or series.

8.4.2.4.1.1 View and filter database information

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Image Database***.

   The ***Manage image database*** screen opens.
5. Expand the ***Filter*** drop-down menu to select filtering criterion (***Patient name***, ***Patient ID***, ***Referring physician name***, ***Modality***, or ***Exam date***).
6. At ***contains***, start typing the patient name, patient ID, etc. you are searching for.
7. Click ***Refresh*** to update the exam list. The table contains a maximum of 200 exams. To view other exams, click on the arrow on the right of ***Exams*** and select a new range.
8. To view additional information associated with an exam or series, click anywhere on the row. The row is highlighted and series or image information is displayed.

8.4.2.4.1.2 Download exams or series

1. To download one or more exams, select the check boxes on the left of the row and click ***Download selected***.

   Selecting the check box to the left of the exam name will not display the series information.
2. If the exam(s) selected for download contain(s) patient information, the system displays the following prompt:

   ```
   Image data contains sensitive patient information. Use anonymization
   if patient data is not needed.
   ```

   - Click ***Anonymize and download*** to download the exam(s) with anonymized patient information.
   - Click ***Download selected*** to download the exam(s) without anonymization.
   - Click ***Cancel*** to cancel the download process.

8.4.2.4.1.3 Delete exams or series

1. To delete one or more exams, select the check boxes on the left of the row and click ***Delete selected*** and ***OK***.

   Selecting the check box to the left of the exam name will not display the series information.
2. To delete specific series within an exam, click anywhere in a single row in the exam group. The row is highlighted and all series in the exam are displayed in the ***Series*** area.
3. In the series group, click the check box(es) to the left of the series name.
4. Click ***Delete selected*** and click ***OK*** on the verification prompt.

8.4.2.4.2 Displaying and saving image header information

Use this procedure to display and save the header information for images.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Image Database***.
5. Click on a single line entry in the exam area.

   The ***Series*** information is displayed.
6. Click on a single series entry in the ***Series*** area.

   The ***Images*** information is displayed.
7. Select the check box at a single image entry.
8. Click ***Dump header***
9. Save or view the information:
   - To save it, click ***Pull from system*** and ***Save***. Navigate to the desired location on your client and click ***Save***.
   - To view it, click ***Display*** on the information on the screen.

8.4.2.5 Monitoring application usage

You can use the ***Application Usage Monitor*** feature to view your application usage for a given period. Whenever you launch a compatible application with a new exam, the usage is counted. For the actual, complete list of applications for which this feature is available, contact your GE Service Representative.

NOTE

> Some applications do not log their usage. Therefore, check with your local GE representative if the application you purchased is compatible with the ***Application Usage Monitor*** feature.

NOTE

> Application usage is compacted upon time and potentially on the number of usage logs.

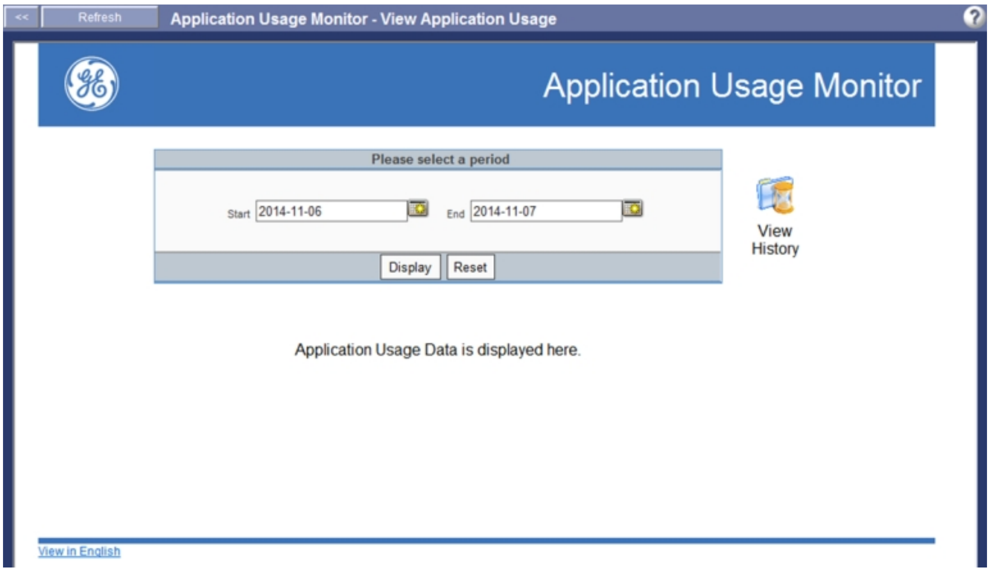
NOTE

> ***Application Usage Monitor*** is available to service and administrator users only.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Administrative***.
3. Click ***Utilities***.
4. Click ***Application Usage Data***.

   The ***Application Usage Monitor - View Application Usage*** screen opens.

Figure 3 Application Usage Monitor - View Application Usage screen



<<
Refresh
Application Usage Monitor - View Application Usage
Application Usage Monitor
Please select a period
Start 2014-11-06
End 2014-11-07
Display
Reset
View History
Application Usage Data is displayed here.
View in English

This screen allows you to view the summary of the application usage for a selected period.

Note that the screen is displayed in the language set for the AW Server. To display the screen in English, click the ***View in English*** link at the bottom left corner of the screen.

5. In the ***Please select a period*** pane, click the calendar icons next to the ***Start*** and ***End*** fields to select the start and end dates.

   The calendar does not allow selecting any date that is more than 2 years prior to the current date.

   You can modify the selected dates by clicking the calendar icons again. Alternatively, click ***Reset*** to clear both fields.

6. Click ***Display*** to view the application usage information for the selected period.

   The ***Application Usage Details of applications between <start date> To <end date>*** table with the columns ***Applications***, ***Count*** and ***Details*** is displayed. Each row contains information about a particular application.

   NOTE

   If data is not available for the selected period, the screen displays the following message:

   ```
   No data available. Please select a different date range.
   ```

7. Click the ***Click here*** link in the ***Details*** column to display usage details for a specific application.

8. Click ***Go Back*** to return to the initial screen (see Figure 3 on page 69).

To view usage history:

1. Click the ***View History*** icon to display application usage history.

NOTE

If usage history data is not available, the screen displays the following message:

```
No Application Usage History data found.
```

In this case, click ***Go Back*** to return to the initial screen.

2. Select a year in the ***Year*** drop-down menu.

   Application usage history data can be displayed for 3 years preceding the previous year.

3. Click ***Display*** to view usage summary for the selected year.

8.5 Maintenance

8.5.1 Maintenance mode

The maintenance mode suggests a workflow for an orderly sequence of tasks related to maintaining the system. Once you enter the maintenance mode, a notice is displayed on all tool pages and users are prohibited from logging in. It is important that only one person be in the maintenance mode at one time.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Maintenance***.
4. Click the ***Maintenance guide*** tab for important information about AW Server maintenance.
5. Click the ***Broadcast message*** tab to set up maintenance mode notifications.

   See Broadcasting messages to clients for details on how to use this function.

6. Click ***Start maintenance*** tab.
   a. Use the default or enter a new disconnect message in the ***Disconnect message*** text field.
   b. Click ***Refresh*** to verify that there is no client logged in.
   c. Click ***Start Maintenance***.
   d. Click ***OK*** on the confirmation prompt
   e. Any clients still logged on will see the disconnect message and are immediately logged out. Any work not saved is lost. Whenever possible, it is best to use this feature when there are no clients logged in.
7. Click the ***Maintenance tasks*** tab to view the list of tasks that can only be performed in maintenance mode and those tasks where maintenance mode is not required, but recommended.
8. Having performed the tasks and ensured that there are no Service Tool tasks in progress, navigate back to the ***Maintenance*** > ***Maintenance*** screen and click ***Finish maintenance***.

   The AW Server is put back to normal mode and users can log back in.

NOTE

> Maintenance can be completed with ***Finish maintenance*** only if the current AW Server configuration is valid, otherwise the system will remain in maintenance mode. For details about registering configuration, see Registering configuration.

8.5.2 Adding or updating AW Server software

The version management tools allow you to install or re-install software onto your server. Some software comes preloaded on the AW Server, while other software upgrades may be provided on media from GE. If your system is connected to GE via InSite connections and Software Download is configured by service, software updates are automatically downloaded to the AW Server. When there is new software to be installed a message is posted on the ***HealthPage***.

The left column lists the operating system, platform version and applications currently installed on the server. The right column lists packages available for installation.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Version Management***.

   The ***Server and client side version management*** screen opens.

   The system does not need to be in maintenance mode to view or reject software.

8.5.2.1 Add or update AW Server software procedure

Follow this procedure to install software updates uploaded to the server by GE.

1. Put the system in the maintenance mode (see Maintenance mode).
2. On the ***Server and client side version management*** screen, click the ***Install/Uninstall*** tab.
3. Click ***Hard disk***.
4. Click ***Contents*** to view the available software and applications which are listed on the right side of the screen.

   These upgrades are highlighted in yellow.
5. Click ***Details*** to view a full list of applications in the package.
6. Select the software packages and click ***Install*** to begin. The status tab showing progress is automatically displayed during installation.
   - Any previously installed software application (for example Volume Viewer) is automatically overwritten with the newly installed software. Installing a version of software older than the currently loaded version must be handled by a service engineer.
   - If you click ***Don't install***, the software is tagged as ***Refused***, but still available for installation at a later date.

NOTE

After AW Server and/or applications installation has been completed, the system displays the ***MANDATORY STEP TO FINISH INSTALLATION!*** dialog prompting you to register your configuration. Click ***OK*** on the dialog to close it. See Registering configuration for detailed instructions about registering configuration.

NOTICE

Newly downloaded software may contain important updates and refusal is not recommended.

8.5.2.2 Install preloaded software from a hard disk or CD/DVD

Follow this procedure if you are re-loading software that came with the AW Server.

1. Put the system in the maintenance mode (see Maintenance mode).
2. On the ***Server and client side version management*** screen, click the ***Install/Uninstall*** tab.
3. Select the media from which you will install the software:
   - To load directly from the hard disk, click ***Hard Disk***.
   - To load from a CD/DVD, insert the media in the server drive and click ***CD/DVD***.

     Click ***Contents*** to see the available software and applications which are listed on the right side of the screen.
4. Click ***Details*** to view a full list of applications in the package.
5. Select the software packages and click ***Install*** to begin. The status tab showing progress is automatically displayed during installation.

View Release Note Documentation

On the ***Server and client side version management*** screen, click the ℹ to view the release notes for the application.

8.5.2.3 Upload ISO

Follow this procedure to upload an application from hard disk, CD/DVD, etc. in ISO format.

1. Put the system in the maintenance mode (see Maintenance mode).
2. On the ***Server and client side version management*** screen, click the ***Install/Uninstall*** tab.
3. Click ***Upload ISO***.
4. On the ***Send files to system*** dialog that opens, click ***Browse...*** and navigate to the ISO file’s location.
5. Select the ISO file and click ***Open***.
6. Click ***Send to system*** to upload the ISO file or click ***Cancel*** to cancel the operation.

   The uploaded ISO file is stored under `/var/lib/ServiceTools/upload`.

7. Click ***OK*** on the ***Upload successful*** dialog box.

8.5.2.4 Upload DVD Collector

Follow this procedure to upload multiple applications at the same time from hard disk, CD/DVD, etc. in ISO format.

1. Put the system in the maintenance mode (see Maintenance mode).
2. On the ***Server and client side version management*** screen, click the ***Install/Uninstall*** tab.
3. Click ***Upload DVD Collector***.
4. On the ***Send files to system*** dialog that opens, click ***Browse...*** and navigate to the location of the ISO files.

   Note that all ISO files that you want to upload have to be in the same location.
5. Holding down the ***Ctrl*** key, select the ISO files and click ***Open***.
6. Click ***Send to system*** to upload the ISO files or click ***Cancel*** to cancel the operation.

   The uploaded ISO files are stored under **`/var/lib/ServiceTools/upload`**.
7. Click ***OK*** on the ***Upload successful*** dialog box.

8.5.2.5 View install/uninstall status

On the ***Server and client side version management*** screen, click the ***Status*** tab to check the install/ uninstall process status.

8.5.2.6 Activate licenses

1. Put the system in the maintenance mode (see Maintenance mode).
2. On the ***Server and client side version management*** screen, click the ***License Activation*** tab.
3. Click ***Refresh*** to update license status information.
4. Select the check box in front the application(s) you want to activate the license(s) of or click ***Activate available*** to select the applications for which licenses are currently available on the license server.
5. Click ***Apply***.

8.5.3 Registering configuration

Follow this procedure to register configuration if the registration of the AW Server is incomplete or has failed, or any incompatible application is installed.

1. Access Service Tools (see Accessing Service Tools).
2. If the system is not in maintenance mode, put it in maintenance mode (see Maintenance mode).
3. Click ***Maintenance***.
4. Click ***Register Configuration***.

   The ***Register Configuration*** screen opens.

   - If you have a valid Registration Key:

a. Enter the Registration Key at ***Install Registration key*** in the ***Install Registration key*** area.

b. Click ***Register***.

- To register the configuration automatically, click ***Perform Auto Registration*** in the ***Auto Register*** area.

  Note that auto registration is performed without user interaction on ***Finish maintenance*** in the case of InSite check-out.

- If the system is not connected to GE, and valid Registration Key not available, perform manual registration as follows:

  a. Click ***Download Configuration*** in the ***Download Configuration (Manual Registration)*** area to export the configuration file to media (e.g., a USB stick).

  b. Upload this file to https://awcct.gehealthcare.com to get a Registration Key. If you cannot connect from the system, try from a PC with internet access.

  c. Install the Registration Key on the system to enable software/applications:

     i. Enter the Registration Key at ***Install Registration key*** in the ***Install Registration key*** area.

     ii. Click ***Register***.

8.5.4 Backup

8.5.4.1 Backing up system configuration

NOTICE

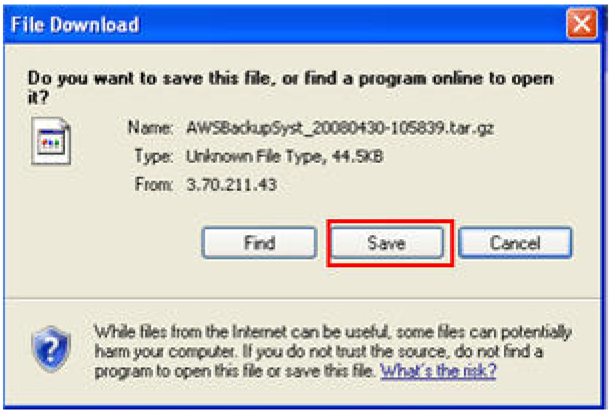
Although not mandatory, this procedure is best done in maintenance mode or when the system is idle. Backing up in a non-maintenance mode may result in a partial backup.

The instructions for backing up preferences on the client refer to the dialog boxes on Microsoft® Internet Explorer®. Different web browsers may have slightly different steps or button names.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Backup***.
4. Click ***System configuration***.

   The ***Backup system configuration*** screen opens.
5. Either select the ***Select as last known good configuration*** check box or select specific items (files or directories) in the list under ***Available configurations***.
6. Click either ***Pull from system*** to save the data on your client or ***Save on system***.
7. If you save on system, the data is saved on a back up location on the server and no further action is required.

Click ***Save*** on the ***File Download*** dialog box.



File Download

Do you want to save this file, or find a program online to open it?

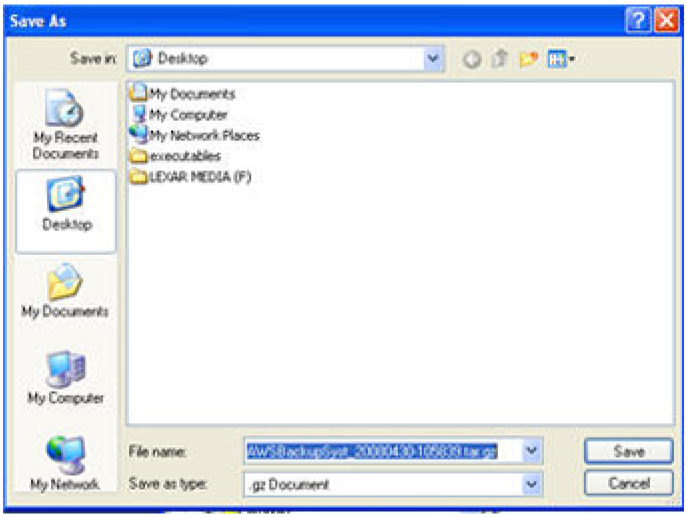
Name: AWSBackupSyst_20080430-105839.tar.gz

Type: Unknown File Type, 44.5KB

From: 3.70.211.43

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

8. Navigate to a location on your client and click ***Save*** on the ***Save As*** dialog box.



Save As

Save in: Desktop

My Documents
My Computer
My Network Places
executables
LEXAR MEDIA (F)

File name: AWSBackupSyst_20080430-105839.tar.gz

Save as type: .gz Document

NOTICE

If you rename the file (which is not recommended), be sure to keep the ".tar.gz" file extension.

9. When the download is complete, click ***Close***.

You can set up automatic backup.

1. In the ***Recurrence*** section of the ***Backup system configuration*** screen, enter the ***Start time*** the backup will begin. Use 24 hour time format.

   The ***Recurrence*** section displays the following information:

   ```
   Recurrence will be performed in non-Maintencance Mode, meaning that
   applications might keep preferences in memory, resulting partial
   backup.
   ```

2. Select the ***daily***, ***weekly*** or ***monthly*** option button to set the frequency of the recurrence of the automatic backup.

3. Click ***Activate***.

   To cancel the automatic backup, click ***Deactivate***.

8.5.4.2 Backing up user preferences

NOTICE

Although not mandatory, this procedure is best done in maintenance mode or when the system is idle. Backing up in a non-maintenance mode may result in a partial backup.

The instructions for backing up preferences on the client refer to the dialog boxes on Microsoft® Internet Explorer®. Different web browsers may have slightly different steps or button names.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Backup***.
4. Click ***User Preferences***.

   The ***Backup user preferences*** screen opens.
5. Under ***Available preferences***, select the check box(es) in front the user(s)' name(s) whose data you want to backup.
6. Click either ***Pull from system*** to save the data on your client or ***Save on system***.
   - If you select ***Save on system***, the data is saved on a back up location on the server and no further action is required.
   - If you select ***Pull from system***:
     a. Click ***Save*** on the ***File Download*** dialog box.
     b. Navigate to a location on your client and click ***Save*** on the ***Save As*** dialog box.

        The file name contains:
        - system ID (if configured)
        - type of download
        - time stamp
        - extension

        NOTICE

        If you rename the file (which is not recommended) be sure to keep the ".tar.gz" file extension.
     c. When the download is complete, click ***Close***.

8.5.5 Restore

8.5.5.1 Restoring system configuration

NOTICE

This procedure must be performed in the Maintenance mode.

8.5.5.1.1 Restore system configuration from the server

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Restore***.
4. Click ***System configuration***.

   The ***Restore system configuration (Maintenance mode is required)*** screen opens.
5. At ***Source***, select one of the following option buttons:
   - ***System*** to see the files saved to the server backup partition.
   - ***Upload*** to restore files saved on the client back to the server (see 8.5.5.1.2 Restore system configuration from the client on page 77).

     NOTE

     The name of the file to be uploaded must contain the string `backupSyst`, otherwise the system will display an error message and the file will not be uploaded.
   - ***Last known good*** to restore the files saved via the ***Last known good configuration*** at system configuration backup.
6. Click ***Refresh*** to ensure the latest files are listed.
7. Select a file in the list below the ***Upload configuration*** button.
8. At ***Available configurations***, select the item(s) you want to recover.
9. Click ***Restore Selected***.

8.5.5.1.2 Restore system configuration from the client

All data must be restored from the AW Server. If you saved data to your client, you must first copy the data onto the server and then restore the data.

The instructions for backing up preferences on the client refer to the dialog boxes on Microsoft® Internet Explorer®. Different web browsers may have slightly different steps or button names.

1. Click ***Maintenance***.
2. Click ***Restore***.
3. Click ***System configuration***.

The ***Restore system configuration (Maintenance mode is required)*** screen opens.

4. Select the ***Upload*** option button.
5. Click ***Upload configuration***.
6. On the ***Send files to system*** dialog that opens, click ***Browse...*** and navigate to the required file's location.

   Optionally, enter checksum information at ***md5 or sha-1 checksum (optional)***.
7. Select the file and click ***Open***.
8. Click ***Send to system*** to upload the file or click ***Cancel*** to cancel the operation.

   The uploaded file is stored under `/var/lib/ServiceTools/upload`.
9. Click ***OK*** on the ***Upload successful*** dialog box.
10. At ***Available configurations***, select the item(s) you want to recover.
11. Click ***Restore Selected***.

8.5.5.2 Restoring user preferences

NOTICE

This procedure must be performed in the Maintenance mode.

8.5.5.2.1 Restore user preferences from the server

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Restore***.
4. Click ***User preferences***.

   The ***Restore user preferences (Maintenance mode is required)*** screen opens.
5. At ***Source***, select the ***System*** option button.
6. Click ***Refresh*** to ensure you see the latest files.
7. Select a file in the list below the ***Upload preferences*** button.
8. Click ***Refresh*** to refresh the list of ***Available preferences***.
9. Select the user whose preferences you want to restore.
10. Click ***Restore Selected***.

8.5.5.2.2 Restore user preferences from the client

All data must be restored from the AW Server. If you saved data to your client, you must first copy the data onto the server and then restore the data.

The instructions for backing up preferences on the client refer to the dialog boxes on Microsoft® Internet Explorer®. Different web browsers may have slightly different steps or button names.

1. Click ***Maintenance***.
2. Click ***Restore***.
3. Click ***User preferences***.

   The ***Restore user preferences (Maintenance mode is required)*** screen opens.
4. Select the ***Upload*** option button.

   NOTE

   > The name of the file to be uploaded must contain the string `backupSyst`, otherwise the system will display an error message and the file will not be uploaded.
5. Click ***Upload preferences***.
6. On the ***Send files to system*** dialog that opens, click ***Browse...*** and navigate to the required file's location.

   Optionally, enter checksum information at ***md5 or sha-1 checksum (optional)***.
7. Select the file and click ***Open***.
8. Click ***Send to system*** to upload the file or click ***Cancel*** to cancel the operation.

   The uploaded file is stored under **`/var/lib/ServiceTools/upload`**.
9. Click ***OK*** on the ***Upload successful*** dialog box.
10. Select a file in the list below the ***Upload preferences*** button.
11. Click ***Refresh*** to refresh the list of ***Available preferences***.
12. Select the user whose preferences you want to restore.
13. Click ***Restore Selected***.

8.5.6 Network

8.5.6.1 Overview

NOTICE

This procedure must be performed in the Maintenance mode.

You can manually enter the IP address, default gateway and host name. If this information is not known, it can be obtained from the site administrator or IT department.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Maintenance***.
3. Click ***Network***.

   The ***Perform network configuration (Maintenance mode is required)*** screen opens and displays the following message:

```
While the Service Tools is used remotely through network it is highly
recommended to set a known configuration. By modifying network
settings the system might be unavailable from a remote station.
```

The screen contains the following tabs:

- ***IP address, Default gateway***
- ***Hostname***
- ***DNS settings***
- ***Firewall rules***

8.5.6.2 IP address, Default gateway tab

1. Click the ***IP address, Default gateway*** tab to configure the IP address and default gateway.
2. In the ***Network interfaces*** area, click ***Refresh interface info***.
3. In the ***Configure system IP address*** area, select/enter:
    - the network interface (select the interface in the ***Network interfaces*** drop-down menu),
    - ***IP address***,
    - ***Netmask***.

   Click ***Check IP*** to verify the network (TCP/IP) connection.
4. In the ***Routing table*** area, click ***Refresh routing table*** to update the routing table information.
5. In the ***Routes file*** area, click ***Refresh routes*** to update routes information.
6. In the ***Configure default gateway*** area, click ***Check IP*** to verify the network (TCP/IP) connection.
7. Click ***Apply*** to save the configuration or click ***Cancel*** to discard the changes.

8.5.6.3 Hostname tab

1. Click the ***Hostname*** tab to configure the system host and domain name.
2. In the ***Hosts file*** area, click ***Refresh hosts*** to update the host information.
3. In the ***Configure system host name*** area, enter the ***Hostname*** and the ***Domain name***.
4. Click ***Apply*** to save the host and domain name or click ***Cancel*** to discard the changes.

8.5.6.4 DNS settings tab

1. Click the ***DNS settings*** tab to configure the name servers and domain search.
2. In the ***Name server configuration*** area, enter ***Name server IP 1***, ***Name server IP 2*** and ***Name server IP 3*** addresses.

   Click ***Check IP*** to verify the network (TCP/IP) connection.
3. In the ***Domain search configuration*** area, enter ***Domain name 1***, ***Domain name 2*** and ***Domain name 3***.
4. Click ***Apply*** to save the host and domain name or click ***Cancel*** to discard the changes.

Click ***Refresh*** to update the lists.

8.5.6.5 Firewall rules tab

1. Click the ***Firewall rules*** tab to view the firewall rules.
2. In the ***Firewall rules*** area, click ***Refresh firewall info*** to update and display the current firewall settings.

8.6 Tools

8.6.1 Rebooting the server

NOTICE

Rebooting the server will cause users to lose all unsaved work, it is best to perform this function in the Maintenance mode.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Tools***.
3. Click ***Reboot***.

   The ***Reboot*** screen opens.

   The screen displays the list of the tasks that are in progress (if applicable) and the following warning:

   ```
   Warning: Reboot WILL DISCONNECT ALL USERS and ANY ACTIVE SESSION DATA
   WILL BE LOST!
   ```

   ```
   Entering Maintenance Mode first is strongly recommended
   ```

   ```
   Please check the mount count and next file check date on Healthpage
   before rebooting the system.
   ```

   Click one of the available buttons to perform the required action:

   - ***Reboot AW Server***
   - ***Reboot AW Server with File system check***
   - ***Shut down AW Server***

4. Click ***Yes*** on the confirmation prompt.

8.6.2 Importing preferences manually

The preference manager allows users to share preferences/protocols from other users, eliminating the need for each user to re-create the new preferences/protocols from colleagues.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Tools***.

3. Click ***Preferences***.
4. Click ***Manual import***.
5. In the list under ***Select user you want to import preferences from***, select the radio button in front of the user's name you want to import preferences from.

   Optionally, click ***Refresh*** to update the list of available users.
6. A list opens containing all available preferences of the selected user. The listed preferences are selectable one by one arbitrarily or all together.

   To select or deselect all preferences in the list, select or deselect the check box in the top left corner of the list.

   NOTICE

   The preferences/protocols that are new to the importing user are pre-selected by the application. Already existing protocols are not selected automatically and are marked with ***Yes*** in the ***Already exists*** column. When an already existing preference is selected for import, the message ***Yes*** changes to ***Overwrite*** and the selected preference will be overwritten by the new one. Use this with caution as you may lose preferences or protocols!
7. Click ***Import*** to import the preferences from the selected users.
   - Any preference you do not have will be added to your preferences.
   - A summary showing the imported preferences is displayed.

NOTE

In the summary, ***Skipped*** status is displayed if preferences were not imported in order to preserve existing preferences.

NOTE

To avoid inconsistencies in user preferences, ensure all relevant users are logged out during the import process.

8.6.3 Sharing preferences

Chief radiologists and/or other lead professionals can set up best practice preferences sets and have users assigned to these preferences.

NOTICE

Once you have shared your preferences, existing preferences of assigned users will be overwritten by your share. Be aware that updated preferences might contain changes to default measurement units, behavioral settings, etc. Make sure that you describe each important detail of your preferences for the users.

NOTE

Close all running applications before sharing your preferences.

When you have finished setting up the preferences (protocols, measurements, etc.), follow the below procedure to share your current preferences:

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Tools***.
3. Click ***Preferences***.
4. Click ***Share preferences***.

   The ***Share your preferences*** screen opens.
5. In the upper, editable text field on the ***Share your preferences screen***, provide a detailed description of the shared preferences.

   The lower ***History*** field shows the history of the share updates in chronological order.
6. Click ***Share*** to share your preferences or leave the screen to discard changes.
7. Contact your site administrator to assign users to your share if no users have been assigned or you want to have additional users assigned to the share.

Assigned users will automatically get the shared preferences on the next login.

When a new preference share is available, the system will display the ***Automatic preference update notification*** dialog to the assigned users on their next login, with the description of the preferences in the share, and informing them that the updated preferences might contain changes to default settings (measurement units, behavioral and other settings, etc.), also advising them to contact the share owner and the site administrator if the preference update was not communicated in advance. Note that the preference synchronization may take a few minutes.

Once the synchronization is completed, the ***OK*** button becomes active. Click it to close the dialog.

8.6.4 Assigning users to preference shares

When a chief radiologist and/or lead professional shares his/her preferences, the site administrator has to assign users to the share.

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Tools***.
3. Click ***Preferences***.
4. Click ***User-share assignment***.

   The ***Manage user assignments to preference shares*** screen opens, which contains the ***Users sharing***, ***Assigned users*** and ***Users*** columns.

   The ***Users sharing*** column lists the available shares.

   The ***Assigned users*** column displays the users assigned to the share selected in the ***Users sharing*** column.

   The ***Users*** column shows all users. Note that only users who have previously logged in the AW Server at least once are listed.

Click ***Refresh*** in the upper left corner to display the current status of the user list and the shares.

- To display users assigned to a share, click on the share's name in the ***Users sharing*** column. Users assigned to the selected share are shown in the ***Assigned users*** column.
- To assign user(s) to a share:
  a. Click to select the share's name in the ***Users sharing*** column to which you want to assign user(s).

  b. Select the user(s) in the ***Users*** column you want to assign to the selected share.

  Select the ***Only unassigned users*** check box below the column to lists only users who have not been assigned to any share yet.

  To select multiple users, hold down the ***Control*** key and click on each user you want to assign to the share. To select a set of consecutive users, hold down the ***Shift*** key, click on the first, and then on the last user in the list.

  NOTE

  Each user can be assigned to only one share.

  c. Click the **<<** button to assign the user(s) to the share.

  The user(s) are added to the ***Assigned users*** column.

  If you have selected users already assigned to another share, the system displays an ***Alert*** prompt, informing you that certain user(s) is/are already assigned to another share, and whether you want to reassign the user(s) to the currently selected share. Click ***Yes*** to reassign such user(s), or click ***No*** to discard the changes.
- To remove user(s) from a share:
  a. Click to select the share's name in the ***Users sharing*** column from which you want to remove user(s).

  b. Select the user(s) in the ***Assigned users*** column you want to remove from the selected share.

  c. Click the **>>** button to remove the user(s) from the share.

  The user(s) is/are removed from the ***Assigned users*** column and added to the ***Users*** column.

5. Click ***Apply*** to confirm, or click ***Cancel*** to discard the changes.

8.7 Viewing user manuals

1. Access Service Tools (see Accessing Service Tools).
2. Click ***Documentation***.
3. Click ***Documentation***.

   The ***User and service documentation*** screen opens.
4. On the ***User and service documentation*** panel, click the ***Documentation*** button.
5. On the navigation pane on the left side of the window that opens, click the name of the documentation you want to view.

Chapter 9 Troubleshooting Tips

9.1 Troubleshooting tips

NOTE

In the case of problems not discussed herein, contact your site IT Administrator or GE service representative for assistance.

Problem	Solution
Cannot see all the system tools.	Service tools accessibility depends on user (limited, standard, administrator) privileges.
Get the following message: `Login Failed. IP address is not an`	Verify and retype the IP address.
Cannot connect. Get the following message: `Connection failed for unknown reason`	• Verify IP address and re-type the user name and password. • Check network connection.
Maximum number of slices exceeded.	The sum of the number of slices to be loaded and the number of slices already in use exceeds the amount of slices allowed. In this case, close running application(s) to release slices so that resources become available.
Application could not be started.	• Depending on the AW Server integration mode, each client can run a maximum of: • 4 applications (with ***Worklist Browser***) • 5 applications (without ***Worklist Browser***) Close one of the applications to continue. • Log out and log back in. Wait approximately 30 seconds before trying to start application from desktop.
The connection to the server has been closed.	• System was inactive for a predetermined time set by the administrator. • Network connection failed.
System is slow.	• Check network connection and bandwidth. • Verify the network latency is less than identified in data sheet. • Run the network check of the ***Client Checker Tool***. • Check compression ratio.
You cannot launch an application via the client.	Check the amount of RAM on your client. The application will not start with insufficient RAM.

(continued)	
Problem	**Solution**
East Asian languages (Chinese, Japanese and Korean (CJK)) are not displayed properly.	Contact your site IT Administrator for assistance.
All system configuration information is displayed in red in the ***HealthPage***.	You have entered a *Hostname* for your system which includes only numbers or starts with a digit, for example: **1234567** Replace the chosen hostname by a hostname that includes also alphanumerical characters, for example: **AW1234567**
AW Server Hostname is displayed in red in the ***HealthPage***.	The Hostname is limited to 12 characters. Choose another hostname with not more than 12 characters.
If Antivirus or Security Suite software is installed on the client's host operating system (Windows), when you run the AW Server Client, some or all of the following symptoms may occur: • You cannot display an exam series or open any application. • Under the orange icon it indicates that the remote display is disconnected. • Attempts to log out from the client fail – you need to close the client via Windows Task Manager (***Ctrl+Alt+Del***).	Due to the great diversity, it is not possible to give a comprehensive list of all the Antivirus/Security software products which may cause conflicts with the AW Server Client. However, the following products are known to cause these problems: • Trend Micro™ Antivirus products • McAfee® Antivirus/Security products If an Antivirus/Security software product is installed on the workstation try the following first to see whether the symptoms still occur: • temporarily disable it, • reduce the security scan/vigilance level (for instance from High to Medium). Many Antivirus/Security software products provide a tool for "Whitelisting" trusted applications/processes. Check whether this is the case for the product used by the site, and if so, use it to add the following processes to the ***WhiteList*** > ***Trusted*** > ***Safe Application*** > ***Exclusion*** list: • `solo.exe` • `solo32.exe` • `solomini.exe` • `nxproxyGEAWE.exe`

(continued)

Problem	Solution
	You may need to give full paths to these executables. It may be the case that you need to manually add these processes to a White List via the Windows Registry (as in the example below). Note that it may be necessary to temporarily disable Antivirus/Security software before making changes to the workstation's configuration/Registry, and to then re-enable and/or reboot it afterwards. ***NOTICE*** Always consult your site IT Administrator before making changes to workstation configurations, especially if these affect security. **Example of solution for Trend Micro Antivirus** Modify the Windows Registry, adding the following two processes used by the AW Server Client to the antivirus WhiteList: • `[HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC\TmProxy\WhiteList\GEPACS02] "ProcessImageName"="solo.exe"` and • `[HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC\TmProxy\WhiteList\GEPACS] "ProcessImageName"="nxproxyGEAWE.exe"` 1. Press ***Windows key+R***. The ***Run*** dialog box opens. 2. In the ***Run*** dialog box, enter **`regedit`** in the ***Open*** box and press ***OK***. The ***Registry Editor*** opens. 3. In the ***Registry Editor***, navigate to the key folder: ***HKEY_LOCAL_MACHINE*** > ***SOFTWARE*** > ***TrendMicro*** > ***NSC*** > ***TmProxy*** > ***WhiteList***. 4. Right-click the ***WhiteList*** key folder and select ***New*** > ***String Value***. 5. Click on the new key, right-click on the right window panel, select new string value, and then name it **`ProcessImageName`**. 6. Right-click the `ProcessImageName` and select ***Modify*** in the context menu. 7. Enter the process name **`nxproxyGEAWE.exe`** in the ***Value data*** field. 8. Click ***OK***. 9. Repeat the above procedure for the `GEPACS02\solo.exe` key. Your ***WhiteList*** should now contain the new ***GEPACS*** and ***GEPACS02*** keys. 10. Close the ***Registry Editor***.

(continued)

Problem	Solution
	NOTE It is strongly recommended that you reboot the workstation after having made changes to the Registry.
Successfully exported data to a Windows directory, but later you cannot find the data in the directory you saved it in.	It is recommended that you export data only to directories to which you have full write and read permissions. Previously saved data may be found in the Windows `VirtualStore` directory.
The following message is displayed upon launching the ***Client Checker***: `Application Blocked by Security Settings`	**Solution 1:** 1. Open the ***Control Panel***. 2. Click ***Java***/***Java (32 bit)*** to open ***Java Control Panel***. 3. Click the ***Security*** tab. 4. Change the ***Security Level*** to ***Medium***. 5. Click ***Apply***. 6. Click ***OK***. **Solution 2:** 1. Perform steps 1 through 3 above. 2. Click ***Edit Site List...*** to open the ***Exception Site List*** dialog. 3. Click ***Add*** and enter the IP address of the AW Server. 4. Click ***OK***. 5. Click ***Continue*** on the ***Security Warning – HTTP Location*** dialog to add the IP address to the exception site list. Alternatively, click ***Cancel*** to discard the changes. 6. Click ***OK*** on the ***Security*** tab. **Solution 3:** 1. Open the ***Control Panel***. 2. Click ***Java*** to open the ***Java Control Panel***. 3. Click the ***Advanced*** tab. 4. Deselect ***Use SSL 2.0 compatible ClientHello format*** under ***Advanced Security Settings***. 5. Click ***Apply***. 6. Click ***OK***.
Opening application documentation when using AW Server in Internet Explorer® 10 (or earlier) terminates active Centricity RIS session in hybrid integration mode.	Deselect the ***Reuse windows for launching shortcuts*** option at ***Internet Explorer*** > ***Tools*** > ***Internet Options*** > ***Advanced*** > ***Browsing***.
In case of integration with 3rd party DICOM hosts only:	

(continued)

Problem	Solution
Application launch fails.	**Solution 1:** 1. Access Service Tools. 2. Click ***Adminisitrative***. 3. Click ***Configuration***. 4. Click ***DICOM Hosts***. 5. Select the remote host that is being used and click the ***Check DICOM*** button. If the check is not successful, resolve the network connectivity issue first. **Solution 2:** 1. Access Service Tools. 2. Click ***Adminisitrative***. 3. Click ***Configuration***. 4. Click ***DICOM Hosts***. 5. Select the remote host that is being used and check the following settings: a. ***Allow speed-up of C-FIND query***: If application launch fails, try a different selection. E.g. ***Relational C-FIND*** is supported by Enterprise Archive remote hosts, but other remote hosts may not support it. b. ***Allow early response for C-STORE***: Early response works with Enterprise Archive remote hosts and accelerates data transfer and application launch time. If application launch still fails, after having tried item (a), then try unchecking this option.
Application launches, but the time to display the data or data transfer from the remote host are slow.	**Solution 1:** The bandwidth between the AW Server and the remote host may be too low or the latency may be too big. Check if the bandwidth can be improved or if the latency can be decreased. Suggested values are: • bandwidth: ≥ 1Gbit/s • latency: < 10ms

(continued)	
Problem	**Solution**
	Solution 2: 1. Access Service Tools. 2. Click ***Adminisitrative***. 3. Click ***Configuration***. 4. Click ***DICOM Hosts***. 5. Select the remote host that is being used and check the following settings: a. ***Preferred compression format***: Select ***Automatic*** (default). If image data loading is still slow, select the compression used by this DICOM host to store the images. If e.g. the remote host stores images in one compression format, but here a different compression format is selected, this can degrade the image data loading speed. b. ***Allow early response for C-STORE***: Select this option to speed up the retrieval of images. Turn it off, if application launch fails.
Application launch (the time to create the new tab) is slow for studies with great number of series and images.	1. Access Service Tools. 2. Click ***Adminisitrative***. 3. Click ***Configuration***. 4. Click ***DICOM Hosts***. 5. Select the remote host that is being used and check the following setting: ***Allow speed-up of C-FIND query***: Select ***Relational C-FIND*** if it is supported by this remote host (e.g. Enterprise Archive). Otherwise, select ***Multi-value UIDs for C-FIND*** (default) which also accelerates the C-FIND query.

Chapter 10 Appendices

10.1 AW Server compression types

There are three basic types of compression on the AW Server:

- transfer compression
- display compression (lossless and lossy compression) used during transient states such as rotation, roaming, paging and cine
- data export data compression

10.1.1 Transfer compression

The compression setting on the Tools tab affects how quickly the exam data and images for the preview pane and 2D Viewer are transferred between the server and your client. On a slow or congested network, compressing data may allow for a quicker transfer. However due to the time it takes to compress and uncompress data, if you are working on a fast, relatively uncongested network (i.e. 1GB) , turning compression off may provide the fastest transfer time. The images are always displayed uncompressed without any loss of data or information. The compression is either on or off in the 2D Viewer.

10.1.2 Display compression

The compression setting on the AW Server desktop determines the speed at which you can perform manipulations such as rotations. The greater the compression, the faster the data can be manipulated, but poorer the image resolution. The reduction of image quality with lossy compression may result in a corresponding loss of information content of the images: blurring of fine body structures, loss of small detail, contour effects, etc.

Setting the compression on the AW Server desktop will apply the compression ratio only during transient states such as rotation, paging, roaming or cine in all applications except 2D Viewer and Filmer. During all other times, images are displayed at full fidelity. This compression will NOT apply to data export or the Filmer or 2D Viewer applications.

Compression	Speed	Resolution
High	Faster	Lower
Low	Slower	Higher

NOTE

Any DICOM save or print is performed in full fidelity.

Lossless and lossy compression

- **Lossless** compression uses compression algorithms that allow the original data to be reconstructed from the compressed data. All the information in the acquired data still exists and can be completely reconstructed.

- **Lossy compression** reduces data by eliminating certain information, especially redundant information and results in loss of fine detail or blurring of data.

10.1.3 Data Export compression

The compression setting in data export allows you to make trade offs between image quality and transfer, storage and display rates.

An image quality level of 10 corresponds to maximum image quality (lossless compression), levels from 9 to 1 corresponds to a progressively lower image quality (lossy compression).

10.2 Configuring AW Server host IP addresses at AW Server client installation

AW Server offers an option to provide a list of IPv4 addresses or fully qualified domain names (FQDN) at AW Server client installation that will appear in the host selection drop-down list of the client login screen in alphabetical order.

NOTE

This option is not available in seamless integration mode with a Universal Viewer client.

To provide the list of IP or FQDN addresses:

1. Download the AW Server client (see 6.2 Downloading client on page 33).
2. Do not click ***Run*** on the ***File Download - Security Warning*** dialog box!

   Instead, open a command window as administrator and execute the silent installation command with the **IPLIST** parameter, as shown in the example below:

   ```
   msiexec /i C:\Users\<user>\Desktop\AWS-3.2-SoloInstaller.msi /l*vx %TEMP%
   \install.log IPLIST="3.249.70.237,3.249.70.238" /qn
   ```

   In the **IPLIST** parameter, enter the IP addresses (or FQDNs) you want to add to the host selection list, separated by commas.

   NOTE

   Silent installation returns immediately but works longer in the background.

After the installation process, an `install.log` file will be created in the specified folder that contains information about valid or invalid **IPLIST** items.

- If the **IPLIST** parameter is not specified during installation, and there was a client installed previously, the client will reuse the earlier IP list.
- If the **IPLIST** parameter is specified during installation, the client will disregard the previous IP list (if it existed).

NOTE

After the first successful login, the client saves and memorizes the AW Server host selected and will display this host as default the next time the client is started.