

AW Server 3.2

Advanced Service Manual



5771771-8EN
Revision 9
© 2023 General Electric Company
All rights reserved.

Legal Notes

Trademarks

All products and their name brands are trademarks of their respective holders.

- GE and the GE Monogram are trademarks of General Electric Company.
- Advantage Workstation, InSite and RSvP are trademarks of General Electric Company or one of its subsidiaries.
- AW Server is a trademark of General Electric Company or one of its subsidiaries.
- Microsoft, Windows, the Windows logo and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- UNIX is a registered trademark of The Open Group.
- Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Mozilla and Firefox are registered trademarks or trademarks of Mozilla Foundation in the United States and/or other countries.
- Intel, Core, Pentium, and Xeon are trademarks are trademarks of Intel Corporation.
- Sun, the Sun logo, Sun Fire, Java and Javascript are trademarks or registered trademarks of Oracle, Inc. in the U.S. and certain other countries.
- HP, HEWLETT-PACKARD and the HP Logo (shown below) are registered trademarks that belong to Hewlett-Packard Development Company, L.P.
- VMware and VMware vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other countries.
- DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

Omissions & Errors

Customers, please contact your GE Sales or Service representatives. GE personnel, please use the TrackWise Process to report all omissions, errors, and defects in this publication.

Copyrights

All Material Copyrighted (c) by the General Electric Company, All rights reserved.

Damage in Transportation

All packages should be closely examined at time of delivery. If damage is apparent write "Damage In Shipment" on ALL copies of the freight or express bill BEFORE delivery is accepted or "signed for" by a GE representative or hospital receiving agent. Whether noted or concealed, damage MUST be reported to the carrier immediately upon discovery.

The following process is for North America only (US + Can)

- Note damage on the carrier's delivery paperwork
- Take pictures of damage
- For Equipment damage: Follow Process & Complete Damage / Loss Claim Form

- Timing: No more than 7 days after delivery
- For Property damage: Complete Delivery Incident Form
 - Timing: No more than 2 days after delivery
 - Email with supporting pictures and all paperwork to @HEALTH Claims-Traffic (Claims-Traffic@med.ge.com) or Fax to 262.312.1183 Att: Claims.
- Delivery issues: Complete Delivery Incident Form

Timing: No more than 2 days after delivery

Electrical Contractors

Certified Electrical Contractor Statement

All electrical installations that are preliminary to positioning of the equipment at the site prepared for the equipment shall be performed by licensed electrical contractors. In addition, electrical feeds into the Power Distribution Unit shall be performed by licensed electrical contractors.

Other connections between pieces of electrical equipment, calibrations, and testing shall be performed by qualified GE Medical personnel. The products involved (and the accompanying electrical installations) are highly sophisticated, and special engineering competence is required. In performing all electrical work on these products, GE will use its own specially trained field engineers. All of GE's electrical work on these products will comply with the requirements of the applicable electrical codes.

The purchaser of GE equipment shall only utilize qualified personnel (i.e., GE's field engineers, personnel of third-party service companies with equivalent training, or licensed electricians) to perform electrical servicing on the equipment.

WEEE Directive



This logo applied on GEHC hardware marks it as WEEE (Waste Electrical and Electronic Equipment) compliant according to the EU WEEE directive (2012/19/EU).

This information (product disassembly instructions) is posted on the Hewlett Packard web site at:

<http://www.hp.com/hpinfo/globalcitizenship/environment/productdata/disassemblyservers.html>

These instructions may be used by recyclers and other WEEE treatment facilities as well as HP OEM customers who integrate and re-sell HP equipment.

Revision History

Engineering revisions and master for this document are archived in MyWorkshop as **DOC1955901**.

Release of this document is referenced and archived in TechPub as **5771771-8EN**.

Refer to [AW Server 3.2 documentation on page 22](#) for other documentation references.

Revision	Date	Reason for change
1	November 13, 2020	<p>Initial release for AW Server 3.2 Ext. 4.0: SPR HCSDM00634636.</p> <p>Update workaround for EA3 authentication using SSL connection with Active Directory: SPR HCSDM00621786</p> <p>Update to configure the AE Title separately from hostname on the AW Server: SPR HCSDM00621166</p> <p>Update for CoLA license server cybersecurity support: SPR HCSDM00624298</p> <p>Added workaround for CoLA server not running after software update: SPR HCSDM00633489</p> <p>Added workaround for restore failure if the built-in Floating License server (CoLA) is disabled: SPR HCSDM00634307</p>
2	December 17, 2020	<p>Update workaround to restart the CoLA process: SPR HCSDM00626278</p> <p>Added workaround for Norwegian language support for Solo Client on AW Server Seamless integration mode: SPR HCSDM00637153</p> <p>Added recommendations to avoid Solo Client issues: SPR HCSDM00637148</p>
3	March 5, 2021	<p>Update for ISD migration toward FFA and cleanup: SPR HCSDM00645306</p> <p>Added workaround for the uninstallation of the Advantage SIM application failure: SPR HCSDM00645616</p> <p>Added workaround for CoLA Floating License Cybersecurity issue: SPR HCSDM00644620</p> <p>Added workaround for DDC performance issue: SPR HCSDM00647017</p> <p>Added workaround for cluster certificate application issue: SPR HCSDM00647018</p>
4	October 11, 2021	<p>Update for the introduction of the AW Server 3.2 Ext. 4.2 release: SPR HCSDM00650828</p> <p>Add workaround for the uninstallation of the Advantage SIM application failure: SPR HCSDM00662740</p> <p>Added workaround for backup failure if Advantage SIM is installed: SPR HCSDM00664751</p> <p>Added workaround for Applications launch failure in Hybrid integration mode with the PACS 3rd party integrated AW Server Client: SPR HCSDM00670019</p> <p>Added workaround for the AW Server performance degradation caused by logging out from AW Server Client: SPR HCSDM00662504</p> <p>Update for Certificate Management UI description: SPR HCSDM00672493</p> <p>Added workaround for the Volume Viewer shortcuts executed twice when starting Volume Viewer with Web Access: SPR HCSDM00667250</p>

Revision	Date	Reason for change
5	March 3 rd , 2022	<p>Update for the introduction of the AW Server 3.2 Ext. 4.4 release: SPR HCSDM00677266.</p> <p>Added workaround for the CardIQ Xpress Process 2.3 Ext. 6 application installation failure: SPR HCSDM00675287.</p> <p>Added workaround for the Automatic Configuration Status Summary displaying a failed status in the Healthpage: SPR HCSDM00674782.</p> <p>Added workaround for Registration Status and key invalidation after an upgrade from AW Server 3.2 Ext. 3.2 to Ext. 4.0 or higher: SPR HCSDM00678666.</p> <p>Added workaround for SSL cypher security level being too low on AW Server 3.2 Ext. 4.0: SPR HCSDM00684854.</p> <p>Added workaround for the additional DICOM host appearing when creating or updating a DICOM host on AW Server 3.2 Ext. 4.0 and higher: SPR HCSDM00655915.</p> <p>Added workaround for the issue of the SmartScore custom templates not being saved correctly on AW Server 3.2 Ext. 4.0: SPR HCSDM00684158.</p> <p>Update instructions for Seamless cluster configuration to support 40 k slices per node on versions prior to AW Server 3.2 Ext. 4.4: SPR HCSDM00686301.</p> <p>Added workaround for the service user not being able to download any files provided by the Service tools on AW Server 3.2 Ext. 4.4: SPR HCSDM00688448.</p> <p>Added workaround for the CoLA server not running after software update or system reboot: SPR HCSDM00689260.</p>
6	April 12, 2022	Update to address sdc password issue: SPR HCSDM00693704
7	June 8, 2022	Update for the introduction of the AW Server 3.2 Ext. 4.6 release: SPR HCSDM00692866 HCSDM00696560 HCSDM00700160.

Revision	Date	Reason for change
8	September 21, 2022	<p>Update for the introduction of the AW Server 3.2 Ext. 4.8 release: SPR HCSDM00705950.</p> <p>Added workaround for the Automatic Configuration Status Summary status getting into failure in the Healthpage from AW Server 3.2 Ext. 4.0: SPR HCSDM00673284.</p> <p>Added workaround addressing the renewing of an AW Server external CA signed certificate for versions older than AW Server 3.2 Ext. 4.0: SPR HCSDM00677770</p> <p>Added workaround for the applications temporary lock files issue with SmartScore 4.0 on AW Server 3.2: SPR HCSDM00688305.</p> <p>Added workaround for the Filmer DataExport function being broken on AW Server 3.2 Ext. 4.0 to Ext. 4.8: SPR HCSDM00688310.</p> <p>Added workaround for the System config restore failure and ea3 component corruption on AW Server 3.2 Ext. 4.2 to Ext. 4.8: SPR HCSDM00700274.</p> <p>Added workaround for Application Usage Monitor not working on NanoCloud AW Server on Ext. 3.4 and Ext. 4.0: SPR HCSDM00701196.</p> <p>Added workaround for the Database corruption in Nano-Cloud AW Server: SPR HCSDM00701519.</p> <p>Added workaround for the Scrolling being slow and choppy in Volume Viewer viewport within Universal Viewer on AW Server 3.2: SPR HCSDM00704622.</p> <p>Added workaround for mounted applications USB not working on NanoCloud AW Server from Ext. 4.0: SPR HCSDM00707821.</p> <p>Added workaround for the Certificate Management page issue on AW Server 3.2 Ext. 4.2 to Ext. 4.6: SPR HCSDM00709034.</p> <p>Added workaround for the 3D application not starting after restoring backup containing Web Client settings on AW Server 3.2 Ext. 4.2 to Ext. 4.8: SPR HCSDM00709175.</p> <p>Added workaround for the Platform analytics sweep scripts not getting application usage information from sites on AW Server 3.2 Ext. 4.2 to Ext. 4.6: SPR HCSDM00710445.</p>

Revision	Date	Reason for change
9	February 28, 2023	<p>Update for the introduction of the AW Server 3.2 Ext. 4.9 release: SPR HCSDM00719657.</p> <p>Added workaround for the Service Tools crash after saving anonymous images on AW Server 3.2 Ext. 4.4: SPR HCSDM00711687.</p> <p>Updated the link to the appropriate instruction in the certificate file description (section 3.4.1.3 System Configuration): SPR HCSDM00692190.</p> <p>Added workaround for the Storage red status issue on the Service Tools Healthpage: SPR HCSDM00718715.</p> <p>Added workaround for the Save State created by AW Server applications that cannot be loaded in Micro Cloud on AW Server 3.2 Ext. 4.8: SPR HCSDM00721533.</p> <p>Added workaround for the EAT Audit Trail logs related to the Web Client and next generation applications usage not being visible on the central log server on AW Server 3.2 Ext. 4.8 and Ext. 4.9: SPR HCSDM00717558.</p> <p>Added clarifications for the DICOM AET Port information showing incorrect information in certain integration modes on Service Tools Healthpage: SPR HCSDM00718774.</p> <p>Updated Appendix HP Servers Firmware & BIOS upgrade / patch installation: SPR HCSDM00725641.</p> <p>Updated workaround for the CardIQ Xpress Process 2.3 Ext. 6 application not getting installed correctly on AW Server 3.2 Ext. 4.0 and Ext. 4.2: SPR HCSDM00727584.</p> <p>Added workaround for the 2D datasets that cannot be opened on AW Enterprise systems on AW Server 3.2 Ext. 4.8 and Ext. 4.9: SPR HCSDM00727603.</p>

Contents

Chapter 1 Introduction	26
1.1 Overview	26
1.2 Overview of an AW Server	26
1.2.1 Product Features	28
1.2.2 Upper-Level Functional Description	30
1.2.2.1 Device Description.....	30
1.2.2.2 AW Server terminology	31
1.2.2.3 Virtualization and AW Server.....	31
1.2.3 Network Functional Overview.....	31
1.2.3.1 Computer Network Overview	31
1.2.3.2 Purpose of the Network	31
1.2.3.3 Network Components.....	32
1.2.3.4 LAN vs WAN.....	32
1.2.3.5 Factors in Network Performance.....	32
1.2.3.6 Network Security	32
1.2.3.7 VPN Information	33
1.2.3.8 Default Network Names	33
1.2.4 Client PC Performance.....	33
1.2.5 Remote Service vs. On-Site Service	33
1.2.6 Server Standalone Test - Rationale.....	33
1.2.7 Service Tools HealthPage	33
1.2.8 Network Performance	37
1.2.9 Maintenance Mode.....	39
1.2.10 Groups, Roles and Members.....	39
1.3 Security.....	40
1.3.1 Password Management.....	40
1.3.1.1 Default Passwords.....	40
1.3.1.2 Changing Passwords.....	40
1.3.2 AW Server Extra Security Layer Login.....	41
1.3.3 Patient Confidentiality Notice.....	42
1.3.4 Removal of Image Data	42
1.3.5 Working in an IT Center or Data Center Environment.....	42
1.3.5.1 Security Rules	42
1.3.5.2 Customer IT Security Policy.....	43
1.3.5.3 Physical Security.....	44
1.3.5.4 System Security	44
1.3.6 Authentication Certificate	45
1.3.7 Server Firewall (PNF)	45
1.4 Service Model and Break-Fix Processes.....	46
1.4.1 Introduction - AW Server Installation & Warranty Time Reporting.....	46
1.4.1.1 Installation	46
1.4.1.2 Installed Base In Warranty Costs (IBIW)	46
1.4.1.3 Installed Base Out of Warranty Costs (IBOW).....	46
1.4.1.4 Periodic Maintenance.....	46
1.4.2 Maintenance Roles.....	46
1.4.2.1 Physical AW Servers (GE-supplied)	47
1.4.2.2 "Virtual AW Server" on Customer-supplied Physical Server.....	47
1.4.3 Break-Fix Processes	48

1.5 AW Server System Power-Up Sequence	48
1.5.1 HP DL580/DL560 High Tier Server Power-Down / Power-up Sequence.....	48
1.5.1.1 Power-Down.....	48
1.5.1.2 Power-Up	49
1.5.2 HP DL360 Server Power-Down / Power-up Sequence.....	49
1.5.3 HP ML350 Low Tier Server Power-Down / Power-up Sequence	49
1.5.4 Virtual Machine Power-Down / Power-up Sequence	49
1.5.4.1 Power-up.....	49
1.5.4.2 Power-Down.....	49
1.5.5 Normal— OS Startup/Boot Options.....	50
1.6 Site Pre-installation Specifications	50
Chapter 2 Service Tools.....	51
2.1 Overview	51
2.2 Service Tools Overview.....	51
2.2.1 Service Tools Accounts.....	51
2.2.2 Service Tools Access Privileges.....	52
2.2.3 Logging into Service Tools	53
2.2.4 Service Tools Menu Tree.....	54
2.2.4.1 Navigating in Service Tools	54
2.2.4.2 Refreshing the Service Tools	55
2.3 Initial Configuration menu	56
2.3.1 Remote Service	56
2.3.2 Device Data.....	56
2.3.3 Contact	56
2.3.4 ST Language.....	56
2.3.5 Time Settings (NTP)	57
2.3.6 Database Deletion Settings.....	58
2.3.6.1 Auto Delete Settings.....	58
2.3.6.2 Delete option for worklist browser	58
2.3.7 Configuring SNMP	59
2.3.8 Platform Configuration	62
2.3.9 Licensing	66
2.3.9.1 Activating the preprocessing application (AutoLaunch).....	66
2.3.9.2 MailSender	66
2.3.9.3 CoLA Server Configuration.....	67
2.3.9.4 Floating License Configuration.....	68
2.3.10 Scalability	68
2.3.10.1 Cluster dashboard.....	69
2.3.10.2 Node removal.....	70
2.3.11 Audit Trail (EAT)	71
2.3.12 Prodiag	72
2.3.12.1 Prodiag management with InSite	72
2.3.12.2 Prodiag Management with RSvP	73
2.3.13 GIB Data.....	75
2.3.14 AUM Configuration.....	75
2.4 Administrative Options menu	75
2.4.1 Configuration	75
2.4.1.1 Certificate Management	76
2.4.2 Utilities.....	78
2.4.2.1 Manage Clients.....	78

2.4.2.2 DICOM Network Queue and DICOM Print queue.....	79
2.4.2.3 Image Database.....	80
2.4.2.4 Application Usage Data.....	84
2.5 Tools Menu.....	86
2.5.1 Terminal.....	86
2.5.1.1 How to use the Terminal.....	87
2.5.1.2 Using an ssh client instead of Terminal.....	88
2.5.2 File Transfer Tool	89
2.5.2.1 How to Start the File Transfer Tool.....	89
2.5.2.2 File Transfer from Server.....	90
2.5.2.3 How to use the File Transfer "From Server" Tool – Basic Steps.....	90
2.5.2.4 Selecting the Directory to View	90
2.5.2.5 Communication Status Message	92
2.5.2.6 Directory Contents List.....	93
2.5.2.7 Transferring AW Server Files to Another Location - Procedure.....	93
2.5.2.8 Transferring a File from the Client to the AW Server	94
2.5.3 Shutdown / Reboot.....	96
2.5.3.1 Using Command lines.....	96
2.5.3.2 Using AWS scripts	96
2.5.3.3 Using the Reboot tool.....	97
2.5.3.4 Using the Hypervisor	98
2.5.4 Preferences	98
2.5.4.1 Manual Import	98
2.5.4.2 Share Preferences	99
2.5.4.3 User-share assignment	100
2.6 HP iLO Service Processor.....	101
2.6.1 Overview.....	101
2.6.2 Checking BIOS and Firmware Revisions.....	102
2.6.3 iLO 5 Service Processor for HPE ProLiant DL360 Gen10 Server.....	102
2.6.3.1 iLO 5 Service Processor Setup.....	102
2.6.3.2 iLO 5 Web Interface.....	102
2.6.4 iLO 4 Service Processor for HPE ProLiant ML350p Gen8 Server, HPE ProLiant DL560 Gen8 Server and HPE ProLiant DL360 Gen9 Server	107
2.6.4.1 iLO 4 Service Processor Setup.....	107
2.6.4.2 iLO 4 Web Interface.....	107
2.6.5 iLO 3 Service Processor for HPE ProLiant DL580 G7 Server	113
2.6.5.1 HPE ProLiant DL580 G7 Server Service Processor Setup.....	113
2.6.5.2 iLO 3 Web Interface.....	113
2.6.6 iLO 2 Service Processor for HP ProLiant ML350 G6 Server	118
2.6.6.1 HP ProLiant ML350 G6 Server Service Processor Setup.....	118
2.6.6.2 iLO 2 Web Interface.....	118
Chapter 3 Diagnostics and Troubleshooting	124
3.1 Overview.....	124
3.2 Diagnostic Menu Options.....	124
3.2.1 Floating License	124
3.2.2 License Information	126
3.2.3 Log Files Viewer	126
3.2.3.1 Overview	126
3.2.3.2 Server Log Files	130
3.2.3.3 Client Log Files.....	131
3.2.3.4 Copying the Contents of a Log File.....	131

3.2.3.5 Description of Log Viewer Files.....	131
3.2.3.6 Logfiles list (non-exhaustive)	131
3.2.4 Server and Client Tests.....	138
3.2.4.1 Server Test.....	138
3.2.4.2 AW Server - Client Connectivity Test	139
3.2.5 Network Test.....	140
3.2.5.1 Using the Display Performance Measurement Tool (DPMT)	140
3.2.5.2 Server Network Interface Re-configuration.....	142
3.2.5.3 Firewall Rules Configuration.....	142
3.2.5.4 Routing Tables Configuration.....	142
3.2.6 Network Analyzer	142
3.2.6.1 Function.....	143
3.2.6.2 Testing the Client (Windows®) Operating System.....	144
3.2.6.3 Testing the Client (Linux) Operating System.....	144
3.3 Troubleshooting with FFA.....	144
3.3.1 Retrieving Passwords from FFA.....	144
3.3.1.1 Retrieving the passwords in Insite	144
3.3.1.2 Retrieving the passwords in RSvP.....	144
3.3.2 Accessing Service Tools from FFA.....	145
3.3.3 Accessing iLO from FFA	146
3.3.3.1 iLO cannot be directly accessed from FFA	146
3.3.3.2 iLO can be directly accessed from FFA	147
3.3.4 Troubleshooting with Screen Sharing	147
3.3.4.1 Screen Sharing feature	147
3.3.4.2 Screen Sharing Scenario 1.....	148
3.3.4.3 Screen Sharing Scenario 2.....	150
3.4 General Troubleshooting	153
3.4.1 Understanding the HealthPage	154
3.4.1.1 Hardware Subsystem	156
3.4.1.2 Virtual Machine Status.....	160
3.4.1.3 System Configuration.....	160
3.4.1.4 Version Information	162
3.4.1.5 Configuration and Status.....	162
3.4.1.6 Software Subsystem.....	163
3.4.1.7 Software Subsystems "CORE" Services.....	163
3.4.1.8 Software Subsystem Restart	164
3.4.1.9 Software Subsystems Essential for Service Tools	166
3.4.1.10 Hypervisor hardware not supported.....	166
3.4.2 Basic User Troubleshooting Tips	167
3.4.3 Troubleshooting AW Server Platform / Application Error Messages.....	177
3.4.4 Troubleshooting Seamless Integration.....	183
3.4.4.1 Preprocessing Issues	183
3.4.4.2 Incompatible version of solomini (AWServer client)	183
3.4.4.3 Solomini not found	183
3.4.4.4 3D Applications Button Greyed Out	183
3.4.4.5 Display truncated when using dual screens.....	183
3.4.4.6 Client Windows Flicker.....	184
3.4.4.7 First Connection to Universal Viewer Client	184
3.4.4.8 Poor Performance on Large Screen Systems.....	184
3.4.4.9 AW Server not responding	185
3.4.4.10 Poor Performance After Extended Use.....	185
3.4.4.11 Empty list in Universal Viewer Client.....	185
3.4.4.12 New images.....	185

3.4.4.13 Licensing New Applications on AW Server	185
3.4.4.14 Seamless cluster configuration support with 40k slices per node	185
3.4.5 Tools and tips	186
3.4.5.1 How to Deal with Intermittent Reboot Hangs on Physical Servers	186
3.4.5.2 PING	187
3.4.5.3 Trace Route	187
3.4.5.4 SSH (Secure Shell)	188
3.4.5.5 AW Configuration file (conf)	190
3.4.5.6 Client Checker Tool - Concept	191
3.4.5.7 Network Performance Measurement Tool (command line tool).....	194
3.4.5.8 Display Performance Measurement Tool (command line tool).....	195
3.4.5.9 Troubleshooting Images	197
3.4.5.10 Audit Trail (EAT)	199
3.4.5.11 Checking Logfiles Collected by Problem Report	204
3.4.5.12 MEBEF	205
3.4.5.13 Application Usage Monitor (AUM)	205
3.4.5.14 Antivirus Software on the AW Server.....	205
3.4.5.15 Windows Anti-virus / Security Software on the Client Workstation.....	206
3.4.5.16 Server Firewall (PNF).....	209
3.4.5.17 "awsmonitor" Script	211
3.4.6 AW Server workarounds	213
3.4.6.1 Service Tools window does not resize when Browser window is resized	215
3.4.6.2 Service Tools menu/tab does not display on Firefox	216
3.4.6.3 High Tier Load Failure.....	217
3.4.6.4 Backup/Restore compatibility issue with DICOM hosts.....	217
3.4.6.5 Logfile partition full.....	218
3.4.6.6 AW Server Client login fails due to DLL mistake	219
3.4.6.7 Users disconnected following an unexpected CoLA License Server crash.....	219
3.4.6.8 Remote node control enabled	222
3.4.6.9 Unexpected network traffic sent from AW Server	223
3.4.6.10 Incoming DICOM transfer attempts fail.....	223
3.4.6.11 Cannot save Postscript printer when the IP address contains a 0.....	226
3.4.6.12 Hard drives check command not working on HPE ProLiant DL360 Gen9 Server.....	227
3.4.6.13 DICOM requests (C-FIND) character representation not supported by older systems.....	228
3.4.6.14 AW Server Client login fail due to display error.....	228
3.4.6.15 EA3 authentication using SSL connection with Active Directory not working.....	228
3.4.6.16 AW Server Client connection with the AW Server is lost	229
3.4.6.17 Updating the AE Title following the hostname characters policy change in OS 6.0 (HeliOS 7.7)	230
3.4.6.18 CoLA server not running after software update or system reboot.....	230
3.4.6.19 Restore fails if the built-in Floating License server (CoLA) is disabled.....	232
3.4.6.20 Norwegian language support for Solo Client on AW Server Seamless integration mode.	233
3.4.6.21 DICOM Direct Connect performance issues.....	233
3.4.6.22 Cluster certificate application issue.....	234
3.4.6.23 AW Server Client applications cannot start due to inappropriate user rights on Windows.....	235
3.4.6.24 Outgoing DICOM communication failure (C-FIND, C-STORE).....	236
3.4.6.25 Licenses for applications not installing after an AW Server update or upgrade	238
3.4.6.26 Backup/Restore compatibility issue with AW Server AET port number	239
3.4.6.27 DICOM transfer failure when DICOM Host Access Control change without system restart	240
3.4.6.28 Cannot install the Edison Machine Light and Service outside the GE network.....	240

3.4.6.29 Service/admin user login problems and/or log partition getting full causes system to get unavailable.....	241
3.4.6.30 AW Server on CT Nano-Cloud does not start after CT Console reboot	246
3.4.6.31 Service restart and data loading problems	246
3.4.6.32 Application Usage Monitor not working in NanoCloud AW Server	248
3.4.6.33 Cannot mount USB media on Nano-Cloud	249
3.4.6.34 Database corruption in Nano-Cloud AW Server.....	250
3.4.6.35 Filmer export to PDF function does not work	250
3.4.6.36 EA3 component corruption after system configuration restoration failure.....	250
3.4.6.37 Platform analytics sweep scripts cannot get application usage information from sites	253
3.4.6.38 Login panel is not displayed in Certificate Management page.....	254
3.4.6.39 3D application not starting after restoring backup containing Web Client settings...	256
3.4.6.40 Cannot load Save State created by AW Server applications in Micro Cloud (AW Server hosted by Edison HealthLink).....	256
3.4.6.41 Cannot open 2D datasets on AW Enterprise systems	257
3.4.7 Troubleshooting applications and licenses.....	259
3.4.7.1 Uninstall Node-Locked Licenses	259
3.4.7.2 No licenses displayed in Floating License Manager	260
3.4.7.3 CardIQ Xpress Process does not generate series	261
3.4.7.4 2D Viewer does not launch.....	261
3.4.7.5 System could not supply enough resources for Volume Viewer	262
3.4.7.6 Graphic performance degraded when paging in Volume Viewer	262
3.4.7.7 Applications interactive performance degradation.....	263
3.4.7.8 Dotmed communication causes AW Server performance degradation when loading many volumes in Volume Viewer.....	264
3.4.7.9 Cannot launch applications in Hybrid integration mode with the PACS 3rd party integrated AW Server Client.....	265
3.4.7.10 Logging-out from AW Server Client causes AW Server performance degradation	266
3.4.7.11 Some Volume Viewer shortcuts are executed twice when Volume Viewer is started with Web Access.....	267
3.4.7.12 SmartScore custom templates are not saved correctly	268
3.4.7.13 Scrolling is slow and choppy in Volume Viewer viewport within Universal Viewer	269
3.4.8 Cybersecurity support	270
3.4.8.1 Cyber-attack on the AW Server system	270
3.4.8.2 CoLA license server cybersecurity support.....	271
3.4.8.3 Security vulnerability in Apache's Log4J2 component.....	289
3.4.8.4 SSL cipher security level too low.....	290
3.5 HPE ProLiant DL360 Gen10 Server hardware troubleshooting.....	291
3.5.1 HPE ProLiant DL360 Gen10 Server mechanical components description	291
3.5.2 HPE ProLiant DL360 Gen10 Server system components description	291
3.5.3 HPE ProLiant DL360 Gen10 Server component identification and LED code meaning.....	291
3.5.3.1 HPE ProLiant DL360 Gen10 Server front panel LEDs codes	291
3.5.3.2 HPE ProLiant DL360 Gen10 Server Systems Insight Display LEDs codes	292
3.5.3.3 HPE ProLiant DL360 Gen10 Server hard disk drives LEDs codes.....	292
3.5.4 HPE Insight Diagnostics.....	292
3.5.5 HPE ProLiant DL360 Gen10 Server troubleshooting tips.....	292
3.5.6 Re-configuring the network after a network card replacement	293
3.5.7 Network Card 10Gb/s and virtual switch interaction	293
3.6 HPE ProLiant DL360 Gen9 Server hardware troubleshooting	294
3.6.1 HPE ProLiant DL360 Gen9 Server mechanical components description	294
3.6.2 HPE ProLiant DL360 Gen9 Server system components description.....	294
3.6.3 HPE ProLiant DL360 Gen9 Server component identification and LED code meaning	294

3.6.3.1 HPE ProLiant DL360 Gen9 Server front panel LEDs codes	295
3.6.3.2 HPE ProLiant DL360 Gen9 Server Systems Insight Display LEDs codes.....	295
3.6.3.3 HPE ProLiant DL360 Gen9 Server hard disk drives LEDs codes	297
3.6.3.4 HPE ProLiant DL360 Gen9 Server flex slot battery backup module LEDs and buttons	298
3.6.4 HPE Insight Diagnostics.....	299
3.6.5 HPE ProLiant DL360 Gen9 Server troubleshooting tips.....	300
3.6.6 Re-configuring the network after a network card replacement	300
3.6.7 Network Card 10Gb/s and virtual switch interaction	301
3.6.8 Smart Array P440ar Controller setup error	301
3.7 HPE ProLiant DL560 Gen8 Server hardware troubleshooting	302
3.7.1 HPE ProLiant DL560 Gen8 Server mechanical components description	302
3.7.2 HPE ProLiant DL560 Gen8 Server system components description.....	302
3.7.3 HPE ProLiant DL560 Gen8 Server component identification and LED code meaning	303
3.7.3.1 HPE ProLiant DL560 Gen8 Server front panel LEDs codes	303
3.7.3.2 HPE ProLiant DL560 Gen8 Server Systems Insight Display LEDs codes.....	304
3.7.3.3 HPE ProLiant DL560 Gen8 Server hard disk drives LEDs codes	304
3.7.3.4 HPE ProLiant DL560 Gen8 Server FBWC module LEDs	305
3.7.4 HPE Insight Diagnostics.....	306
3.7.5 HPE ProLiant DL560 Gen8 Server troubleshooting tips.....	307
3.7.6 Re-configuring the network after a network card replacement	307
3.8 HPE ProLiant DL580 G7 Server hardware troubleshooting.....	308
3.8.1 HPE ProLiant DL580 G7 Server mechanical components description	308
3.8.2 HPE ProLiant DL580 G7 Server system components description.....	308
3.8.3 HPE ProLiant DL580 G7 Server component identification and LED code meaning.....	309
3.8.3.1 HPE ProLiant DL580 G7 Server front panel LEDs code meaning	309
3.8.3.2 HPE ProLiant DL580 G7 Server Systems Insight Display LEDs	310
3.8.3.3 HPE ProLiant DL580 G7 Server SAS or SATA hard drive LED combinations.....	311
3.8.3.4 HPE ProLiant DL580 G7 Server FBWC RAID module LEDs code meaning	312
3.8.4 HPE Insight Diagnostics.....	313
3.8.5 HPE ProLiant DL580 G7 Server troubleshooting tips.....	313
3.8.6 Re-configuring the network after a network card replacement	314
3.9 HPE ProLiant ML350p Gen8 Server hardware troubleshooting.....	315
3.9.1 HPE ProLiant ML350p Gen8 Server mechanical components description.....	315
3.9.2 HPE ProLiant ML350p Gen8 Server system components description	315
3.9.3 HPE ProLiant ML350p Gen8 Server component identification and LED code meaning	315
3.9.3.1 HPE ProLiant ML350p Gen8 Server front panel LEDs codes	316
3.9.3.2 HPE ProLiant ML350p Gen8 Server rear panel LEDs codes	316
3.9.3.3 HPE ProLiant ML350p Gen8 Server SAS or SATA hard drive LED codes	317
3.9.3.4 HPE ProLiant ML350p Gen8 Server FBWC module LEDs	318
3.9.4 Troubleshooting HPE ProLiant ML350p Gen8 Server memory problems	319
3.9.5 HPE Insight Diagnostics.....	320
3.9.6 HPE ProLiant ML350p Gen8 Server troubleshooting tips	320
3.9.7 Re-configuring the network after a network card replacement	321
3.10 HP ProLiant ML350 G6 Server hardware troubleshooting.....	322
3.10.1 HP ProLiant ML350 G6 Server mechanical components description.....	322
3.10.2 HP ProLiant ML350 G6 Server system components description	322
3.10.3 HP ProLiant ML350 G6 Server component identification and LED code meaning	322
3.10.3.1 HP ProLiant ML350 G6 Server front panel LEDs code meaning	323
3.10.3.2 HP ProLiant ML350 G6 Server rear panel LEDs code meaning	323
3.10.3.3 HP ProLiant ML350 G6 Server SAS or SATA hard drive LED combinations	324

3.10.3.4 HP ProLiant ML350 G6 Server FBWC for RAID (Flash Backed Write Cache) module LEDs code meaning.....	325
3.10.4 Troubleshooting HP ProLiant ML350 G6 Server memory problems	326
3.10.5 HPE Insight Diagnostics.....	327
3.10.6 HP ProLiant ML350 G6 Server troubleshooting tips	327
3.10.7 Re-configuring the network after a network card replacement.....	328
3.11 HP RAID / Disk Subsystem.....	329
3.11.1 DAS (Direct Attached Storage) for HPE ProLiant DL580 G7 Server / HPE ProLiant DL560 Gen8 Server High Tier	329
3.11.2 RAID / Disk Subsystem Setup Information.....	330
3.11.3 Configuring the HPE ProLiant DL360 Gen10 Server RAID	331
3.11.4 Configuring the HPE ProLiant DL360 Gen9 Server RAID.....	335
3.11.5 Configuring the RAID	339
3.11.6 Various Configuration Checks.....	341
3.12 HPE R/T3000 UPS (Uninterruptible Power Supply).....	342
3.12.1 Overview	342
3.12.2 Purpose	343
3.12.3 How the UPS works	343
3.12.4 UPS Effectivity	343
3.12.5 R/T3000 G2 Front Panel.....	343
3.12.5.1 Front Panel controls	344
3.12.5.2 Front Panel LED indicators	344
3.12.6 R/T3000 G2 Rear Panel	345
3.12.6.1 R/T3000 G2 US/JPN Low Voltage Rear Panel	345
3.12.6.2 R/T3000 G2 International high Voltage Rear Panel	346
3.12.7 Configuring the R/T3000 UPS	346
3.12.7.1 Checking the UPS connection to the utility power.....	346
3.12.7.2 Checking the connection of the devices to the UPS	347
3.12.7.3 Extracting the front bezel and checking the Battery leads connection	347
3.12.7.4 Checking the connection of the UPS ground bonding cable.....	348
3.12.7.5 Checking the connection of the UPS cord retention clips	348
3.12.7.6 Charging the UPS batteries	348
3.12.7.7 Starting power to the load.....	348
3.12.8 Operating the UPS.....	349
3.12.8.1 Initiating a self-test.....	349
3.12.8.2 Silencing an audible alarm.....	349
3.12.8.3 Powering down the UPS	349
3.12.9 Troubleshooting	349
3.12.9.1 Battery mode.....	349
3.12.9.2 Auto-Bypass mode.....	349
3.12.9.3 Updating the UPS firmware.....	350
3.12.9.4 LED troubleshooting.....	350
3.12.10 HP R/T3000 G4/G5 Overview	354
3.12.10.1 Control panel	354
3.12.10.2 UPS operation.....	354
3.12.10.3 Troubleshooting.....	355
3.13 Troubleshooting Virtual AW Server & VMware Platform.....	355
3.13.1 VMware Error Messages.....	356
3.13.2 Each VM Requires a Unique MAC Address	356
3.13.3 Upgrading VMware or Windows	356
3.13.4 VMware Tools - ESXi Server Compatibility.....	356

3.13.5 Ensure VMware Tools Configured for Graceful Shutdown	357
3.13.6 Ensure VMware Hypervisor Configured with Same NTP Server as AWServer VM	357
3.13.6.1 Setup a NTP server for the ESXi server.....	357
3.13.6.2 vSphere Web Client case	359
3.13.7 Windows Memory Management	361
3.13.8 Limitations of Virtual AW Server	361
3.13.9 Virtual disk for images is too small.....	361
3.14 Troubleshooting An Integrated Server	362
3.14.1 Troubleshooting hybrid integration.....	362
3.14.2 Connectivity Limitations in Seamless Integration Mode	362
3.14.3 Troubleshooting Seamless Integration	362
3.14.4 End of Review Setting Lost When Switching Between Full & Seamless Integration.....	363
3.15 Troubleshooting AW Server Clusters.....	363
3.15.1 Single Access to All AW Server Logfiles in a Cluster	363
3.15.2 Number of login allowed in a cluster	366
3.15.3 Troubleshooting HAPS nodes.....	366
3.16 Troubleshooting Client Software.....	367
3.16.1 AW Server Client Logfiles.....	367
3.16.2 AW Server Client supported monitor	367
3.16.3 Known error messages for AWS Client.....	367
3.16.3.1 Maintenance Mode Error message	367
3.16.3.2 Resources Error message	368
3.16.3.3 Display configuration error when trying to launch an application.....	368
3.16.3.4 Windows file and folder access needed to run AWS Client.....	370
3.16.3.5 "Another version of this product is already installed"	370
3.17 Troubleshooting disk encryption	371
3.17.1 Accessing Encryption Manager	371
3.17.2 Clearing Encryption Configuration.....	372
3.17.3 Clearing a Smart Array Controller	373
3.17.4 Master Encryption Key in Local Key Management Mode.....	375
3.17.5 Configuring the Smart Array Controller for Local Key Management Mode	375
3.17.6 Recovering the Crypto Officer Password	377
3.17.7 Lost or forgotten Master Encryption Key.....	378
3.17.8 Replacing an Encrypted Smart Array Controller.....	378
3.17.9 Changing the password recovery settings	378
3.18 Log patterns for log analysis in RMF environments	379
3.18.1 Notifications when disk usage reaches a predefined level	379
3.18.2 Notifications when an error sends audit records to a remote system	379
3.18.3 AIDE logs.....	379
3.18.4 McAfee logs.....	380
3.18.5 Hardware failures.....	381
3.18.6 Apache web server logs.....	381
3.18.7 EAT logs.....	382
3.18.8 Audit logs for monitored syscalls	384
3.18.9 Audit logs for monitored commands	385
3.18.10 GEHC concept template	385
3.18.11 General notes on logs in RMF mode	385
Chapter 4 AW Server Platform Maintenance	388

4.1 Overview.....	388
4.2 Maintenance Mode.....	388
4.2.1 Understanding the Maintenance Mode.....	388
4.2.2 Start Maintenance Mode	389
4.2.3 Maintenance Mode Banner.....	391
4.2.4 Finish Maintenance Mode	391
4.3 Client Broadcast Message.....	392
4.3.1 Broadcast message.....	393
4.3.2 Manage Clients.....	393
4.4 Configuration Backup.....	394
4.4.1 System Configuration Backup	396
4.4.2 User Preferences Backup.....	399
4.4.3 Configuration backup for Clusters.....	401
4.5 Configuration Restore	401
4.5.1 System Configuration Restore	402
4.5.1.1 "System" Radio Button.....	402
4.5.1.2 "Upload" Radio Button	403
4.5.1.3 "Last Known Good" Radio Button	404
4.5.2 User Preferences Restore	405
4.5.3 Final Step after Restore.....	405
4.5.4 Summary of restore behavior.....	406
4.5.5 Configuration restore for Clusters.....	406
4.6 Version Management	406
4.6.1 Version Management Tool Example	406
4.6.2 Version Management Tool	407
4.6.2.1 Install/Uninstall TAB.....	407
4.6.2.2 Status TAB	408
4.6.2.3 Synchronization of Versions on a Cluster.....	409
4.6.2.4 Register Updated Configuration	409
4.7 Network Reconfiguration	409
4.7.1 IP Address, Default Gateway.....	409
4.7.2 Hostname	410
4.7.3 DNS Settings	411
4.7.4 Firewall Rules.....	411
4.7.5 Network Interface Information.....	413
4.8 Database Recovery	414
4.9 Register Configuration	416
4.9.1 Troubleshooting Configuration Registration.....	416
4.9.1.1 Different values for Permanent Key	417
4.9.1.2 Configuration files with no extension.....	417
4.9.1.3 Backup/restore of registration key	417
4.9.2 Configuration Registration command lines.....	417
4.9.2.1 setKey.....	417
4.9.2.2 doAutoRegister	417
4.9.2.3 version.....	417
4.9.3 Configuration Registration logfile	417
4.9.4 Configuration Registration Call Center.....	418
Chapter 5 Software Reload and Client Reinstall	419

5.1 Overview.....	419
5.2 Software Load Process.....	419
5.3 Additional Software Load information.....	420
5.3.1 Load From Cold (LFC) Considerations.....	421
5.3.2 Installation failures.....	421
5.3.2.1 Unsupported Hypervisor Hardware case	422
5.3.3 Platform Licensing.....	422
5.3.4 Product Network Configuration.....	423
5.3.4.1 iLO Configuration (for physical hardware).....	423
5.3.4.2 Server Network Configuration.....	424
5.3.5 Configuration Restore considerations	424
5.3.6 System configuration restore from AW Server 2.0.....	427
5.3.7 User Preferences Restoration.....	428
5.3.8 Registration	429
5.4 OS and AW Server Platform software Service Pack installation	429
5.4.1 Loading the OS and AW Server Platform software Service Pack.....	430
5.4.2 Installing the OS and AW Server Platform software Service Pack.....	432
5.5 AW Server Client Software Upgrades	433
5.5.1 Client upgrade Procedure	433
5.5.1.1 AW Server Client upgrade Procedure on Windows	433
5.5.1.2 AW Server Client for Universal Viewer upgrade Procedure	436
5.5.1.3 AW Server Client Installation Procedure on Linux.....	437
5.5.1.4 Client Monitor screen resolution setup.....	437
5.5.2 Server and Client Installation Validation Tests.....	437
5.5.2.1 Server Stand-Alone TEST	438
5.5.3 Troubleshooting	441
5.5.3.1 Troubleshooting in no integration mode	441
5.5.3.2 Troubleshooting in Seamless integration mode	441
Chapter 6 Planned Maintenance (PM)	443
6.1 Job Card SV001 - Planned Maintenance (PM)	443
6.1.1 Recommended PM Schedule	443
6.1.2 PM Access.....	443
6.1.3 PM Time.....	443
6.1.4 PM Tasks.....	443
6.1.4.1 Check Version Management	444
6.1.4.2 Check the Healthpage.....	444
6.1.4.3 Checking ClamAV® status and logs	444
6.1.4.4 Checking McAfee status and logs	445
6.1.4.5 Verify RMF compliancy.....	445
6.1.4.6 Password change	445
6.1.4.7 Configuration backup	446
6.1.4.8 Check the Scalability page (for cluster only)	446
6.1.4.9 Configuration Registration	446
6.1.5 PM Completion.....	446
6.1.6 Planned Maintenance tasks summary	446
Chapter 7 FRU, Break-Fix and Disassembly /Reassembly Procedures	448
7.1 Overview.....	448
7.2 FRUs (Field Replaceable Units).....	448

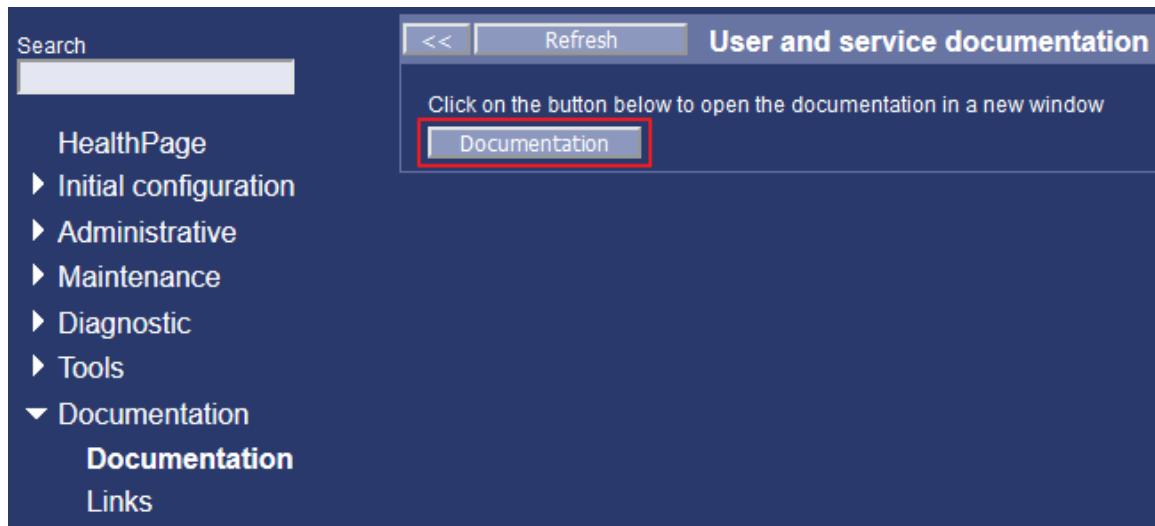
7.3 Break-Fix Processes	448
7.3.1 Responsibility of the hardware break/fix process.....	449
7.3.2 Hardware Vendor Service Support Model.....	449
7.3.3 Service Support Procedures.....	449
7.3.4 HP DL580 / HP DL560 / HP DL360 Hardware - Break-Fix Process.....	449
7.3.5 HP ML350 G6 / ML350p G8 / DL360 G9 Low Tier Hardware - Break-Fix Process	450
7.3.5.1 FRU Labeling Kit.....	451
7.4 HPE ProLiant DL360 Gen10 Server Low Tier Hardware Disassembly/Reassembly Procedures	451
7.5 HPE ProLiant DL360 Gen9 Server Low Tier Hardware Disassembly/Reassembly Procedures.....	452
7.5.1 Electrical Precautions of the HPE ProLiant DL360 Gen9 Server Low Tier.....	452
7.5.2 De-racking the HPE ProLiant DL360 Gen9 Server	453
7.5.3 Replacing HPE ProLiant DL360 Gen9 Server Low Tier Components.....	453
7.5.3.1 HPE ProLiant DL360 Gen9 Server Low Tier high FRU swap	453
7.5.3.2 SAS HDD	453
7.5.3.3 Power Supply	453
7.5.3.4 16GB DDR4 2400 MHz DIMM	453
7.5.3.5 Removing the internal DVD-RW drive.....	453
7.5.3.6 Removing the fan module.....	454
7.5.3.7 System battery.....	454
7.5.4 Re-configuring the network after a network card replacement	454
7.6 HPE ProLiant ML350p Gen8 Server / HP ProLiant ML350 G6 Server Disassembly/Reassembly Procedures	455
7.6.1 LOTO Procedure for HPE ProLiant ML350p Gen8 Server / HP ProLiant ML350 G6 Server	455
7.6.2 Replacing the "hot-plug" power supplies.....	457
7.6.3 Replacing the "hot-plug" hard disk(s)	457
7.6.4 Powering down the server	458
7.6.5 Opening the side cover	458
7.6.6 Replacing the DVD drive.....	458
7.6.7 Replacing the air flow baffles	458
7.6.8 Replacing a cooling fan	458
7.6.9 Replacing the DIMM memory modules.....	458
7.6.10 Replacing the RAID Flash Backed Write Cache module(s)	459
7.6.11 Replacing the Real time clock lithium coin battery	459
7.6.11.1 RTC battery removal.....	459
7.6.11.2 RTC battery replacement	459
7.6.12 Swapping the ML350 CPU box.....	460
7.6.12.1 Field supplied tools.....	460
7.6.12.2 Swap procedure	460
7.7 High Tier Servers Hardware Disassembly/Reassembly Procedures.....	462
7.7.1 Electrical Precautions.....	462
7.7.2 De-racking High Tier Servers.....	463
7.7.3 Replacing High Tier Servers Components	463
7.7.4 Re-configuring the network after a network card replacement	463
7.8 HP Escalation and Communication Flow	464
7.8.1 HP Support Center Web site.....	464
7.8.2 HP supported countries telephone list.....	465
7.9 Hardware Vendor Information Links	465
7.9.1 HP Hardware Vendor Information Links	465
7.9.2 Note about the HP Serial number.....	466

Chapter 8 Other documentation and web links.....	467
8.1 VMware documentation	467
8.2 Web links	467
8.3 Universal Viewer and Centricity PACS documentation.....	467
Appendix A Appendices	469
A.1 Overview	469
A.2 AW Server Licensing	469
A.3 Hardware Vendor Information Links.....	470
A.4 WGET.....	470
A.5 Users, Groups, Roles and Members.....	473
A.5.1 Groups, Roles and Members Example Matrix	473
A.5.2 Example User/Role Matrix	474
A.5.3 Local Users Tab.....	474
A.5.4 Factors to Consider when Creating Local Users Accounts	476
A.5.5 Groups Tab.....	476
A.5.6 "Role" Process Flow for Local Users	478
A.5.7 "Role" Process Flow for Enterprise Users.....	478
A.5.8 Enterprise Tab	478
A.5.8.1 Importing the site's Active Directory server certificate and its Certificate Signing Authority.....	482
A.6 Password Change.....	484
A.6.1 Process Overview	484
A.6.2 Passwords Change Procedure	485
A.6.3 Changing the passwords with FFA.....	485
A.6.3.1 Changing the passwords in Insite	485
A.6.3.2 Changing the passwords in RSvP.....	485
A.7 Setting Date and Time.....	486
A.7.1 Synchronization.....	486
A.7.2 Configuration with Service Tools Time Settings	486
A.7.3 Configuration with Command lines from the terminal.....	487
A.7.3.1 Server Clocks	487
A.7.3.2 Changing the Time and Date using Terminal.....	487
A.7.3.3 Start the Terminal Tool.....	488
A.7.3.4 The "date" Command	488
A.7.3.5 The "hwclock" Command	488
A.7.3.6 How to set the System Clock Time using Terminal	488
A.7.3.7 Setting the Year using Terminal	489
A.7.3.8 Setting the Hardware Clock using Terminal.....	489
A.7.3.9 Changing the System Clock's Time Zone: Do Not Use Terminal	490
A.7.4 Configuration with AWS scripts	490
A.8 Command Line Tools.....	491
A.9 Definitions and Acronyms	493
A.10 Command-Line Interface	495
A.10.1 Command-line Interface.....	495
A.10.2 Getting hardware network information	496
A.10.3 Configuring the network card using command lines (sys-net-conf)	496

A.11 HP ML350 server handling procedure	497
A.11.1 Unpacking procedure	498
A.11.2 Returning procedure.....	498
A.12 Old systems return process after upgrade.....	500
A.13 Filesystem Check.....	500
A.13.1 Filesystem Check feature description	501
A.13.2 Filesystem check Side-effect "issue" description	502
A.13.3 Solutions to minimize the impact.....	502
A.13.3.1 Upgrade to ext4 file system.....	502
A.13.3.2 Check when the next Filesystem check is programmed	502
A.13.3.3 Minimize the impact for the users - Warn the IT Admin asap.....	503
A.13.3.4 Minimize the impact for GEHC FE.....	503
A.14 Launching AWS CLIENT on remote OLE laptop.....	505
A.15 BIOS / FIRMWARE upgrade	506
A.15.1 HP Servers Firmware & BIOS upgrade.....	506
A.15.1.1 Preparation	506
A.15.1.2 Firmware Upgrade.....	509
A.15.2 HP Servers Firmware & BIOS upgrade / patch installation.....	510
A.15.2.1 Installing a server patch.....	510
A.15.2.2 iLO Firmware upgrade.....	510
A.16 HP DL580/DL560/DL360 Handling Procedure.....	511
A.17 Secure Media Destruction Procedure	511
A.18 Application Profiles for AW Server	511
A.19 Re-configuring Corrupted Serial Number	511
A.20 Sun High Tier X4450 returning Procedure	512
A.20.1 Foreword.....	512
A.20.2 Returning procedure.....	513
A.21 Installing/renewing an AW Server external CA signed certificate.....	514
A.21.1 Installing/renewing an AW Server external CA signed certificate - from AW Server 3.2 Ext. 4.2	514
A.21.2 Installing/renewing an AW Server external CA signed certificate - for AW Server 3.2 Ext. 4.0 and older versions	516
A.21.2.1 Procedure	516
A.21.2.2 Revert procedure.....	517
A.22 Hardware Security.....	517
A.22.1 Hardware security - additional setup	517
A.22.1.1 Pre-requisite.....	518
A.22.1.2 HPE ProLiant DL360 Gen10 Server hardware security setup	518
A.22.1.3 HPE ProLiant DL360 Gen9 Server hardware security setup.....	520
A.22.1.4 HPE ProLiant DL560 Gen8 Server hardware security setup.....	521
A.22.1.5 HPE ProLiant DL580 G7 Server hardware security setup	523
A.22.1.6 HPE ProLiant ML350p Gen8 Server hardware security setup.....	524
A.22.1.7 HP ProLiant ML350 G6 Server hardware security setup	526
A.22.2 Removing passwords or recovering from password loss.....	527
A.23 RPM2CPIO	528
A.24 AW Server enhanced security configuration	529

AW Server 3.2 documentation

- For AW Server 3.2 Ext. 3.4 or higher, Service Documentation is available **online only** on:
 - The Customer Documentation Portal for Class A Service Documents:
<https://www.gehealthcare.com/documentationlibrary>
 - SIMS Content Viewer for all Service Documents.
- For previous extensions, in Service Tools, select **Documentation > Documentation**. The *User and service documentation* window displays.



Click on the **Documentation** button. Two pages open to browse the available User and Service documents.

NOTE

The User documents page tiles over the Service documents page. These pages may be updated with new documents when available.

Service documents example: to open a document, click on the corresponding link.

AW Server 3.2 Extension	Manual Name	Part Number
4.9	AW Server 3.2 Advanced Service Manual	5771771-8EN
	AW Server 3.2 Ext. 4.9 Installation Manual	5922979-8EN
	AW Server 3.2 Ext. 4.9 Pre-Installation Manual	5922978-8EN
	AW Server 3.2 Ext. 4.9 Hardware Installation Manual	5922980-8EN
4.8	AW Server 3.2 Advanced Service Manual	5771771-8EN
	AW Server 3.2 Ext. 4.8 Installation Manual	5884093-8EN
	AW Server 3.2 Ext. 4.8 Pre-Installation Manual	5884092-8EN
	AW Server 3.2 Ext. 4.8 Hardware Installation Manual	5884094-8EN
4.2, 4.4 and 4.6	AW Server 3.2 Advanced Service Manual	5771771-8EN
	AW Server 3.2 Ext. 4.2, Ext. 4.4 and Ext. 4.6 Installation Manual	5878563-8EN
	AW Server 3.2 Ext. 4.2, Ext. 4.4 and Ext. 4.6 Pre-Installation Manual	5878562-8EN
	AW Server 3.2 Ext. 4.2, Ext. 4.4 and Ext. 4.6 Hardware Installation Manual	5878564-8EN
4.0	AW Server 3.2 Advanced Service Manual	5771771-8EN
	AW Server 3.2 Ext. 4.0 Installation and Service Manual	5719443-8EN
	AW Server 3.2 Ext. 4.0 Pre-Installation Manual	5719441-8EN
	AW Server 3.2 Ext. 4.0 Hardware Installation Manual	5719442-8EN
3.4 and prior	AW Server 3.2 Advanced Service Manual	5771771-1EN
	AW Server 3.2 Installation and Service Manual	5719443-1EN
	AW Server 3.2 Pre-Installation Manual	5719441-1EN
	AW Server 3.2 Hardware Installation Manual	5719442-1EN

Getting Started

Conventions

Intent of information

The information in this document is designed to support the chapter name and/or process it is found in.

The core sections of the manual are:

- **Chapter 1 - Introduction** - this chapter presents the capabilities of AW Server, and outlines key Service procedures.
- **Chapter 2 - Service Tools** - this chapter explains the on-line Service Tools provided with the AW Server Platform.
- **Chapter 3 - Diagnostics and Troubleshooting** - this chapter provides detailed diagnostics and troubleshooting procedures and tools.
- **Chapter 4 - AW Server Platform Maintenance** - this chapter includes standard maintenance procedures for the AW Server Platform.
- **Chapter 5 - Software Reload and Client Reinstall** - this chapter explains how to upgrade or reinstall AW Server software:

- Load From Cold - reload the whole software (OS + AW Server platform + Volume Viewer Applications + additional Applications)
- Reinstall Client Software
- **Chapter 6 - Planned Maintenance (PM)** - this chapter details the planned maintenance procedures.
- **Chapter 7 - FRU, Break-Fix and Disassembly / Reassembly Procedures** - this chapter explains:
 - The parts and catalog structure of the product, and the Field Replaceable Units.
 - Commonly required physical maintenance procedures
- **Chapter 8 - Other documentation and web links** - this chapter explains how to access external documentation and gives the links to web sites relevant to Service.
- **Appendices** - these sections contain additional technical reference material that goes beyond what may be needed for standard Service procedures.

NOTICE

This manual does not cover the installation and configuration of the AW Server 3.2 product. Installation and configuration of the AW Server 3.2 product is addressed by the AW Server 3.2 Installation and Service Manual and the AW Server 3.2 Hardware Installation Manual.

Identification of software releases

Changes for CFDA rules

Identification of software releases now complies with the CFDA regulations (Chinese Food and Drug Administration). Only the CFDA registered release number is displayed on the User Interface and on the software media (CD/DVD) art-work:

For example: AW Server 3.2, AW Server 3.2 Ext. 1.2, AW Server 3.2 Ext. 2.0...

A corresponding engineering release identifier is displayed by the `conf` command, with the following format: `aws-3.2-x.y`

For example: `aws-3.2-2.0`

This engineering release identifier can also be found in the SW media, in the `release.txt` file.

This change also impacts the Applications and other GEHC products.

Information Disclaimer

The information in this document is accurate at the time of the writing of this document. However, in the future hardware, BIOS, and software revisions may change making some details inaccurate or making the coverage of some details missing. This document may or may not get updated when these changes occur, and may or may not get updated at the exact time of such changes.

Safety Terminology

The terms “danger”, “warning”, and “caution” are used throughout this manual to point out hazards and to designate a degree or level of seriousness. Hazard is defined as a source of potential injury to a person. The terms “important” and “note” are used to indicate other information you should be aware of. Familiarize yourself with the following terminology descriptions:

DANGER

Indicates an imminently hazardous situation which if not avoided, will result in death or serious injury.

WARNING

Indicates a potentially hazardous situation, which if not avoided, could result in death or serious injury.

CAUTION

Indicates a potentially hazardous situation, which if not avoided, may result in a minor or moderate injury.

NOTICE

Indicates information where adherence to procedures is crucial or where your comprehension is necessary to apply a concept or effectively use the product.

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.

Data Entry Formatting Conventions

Certain text formats are used to indicate things such as commands that you type in or keys that you press on the keyboard, etc. For example:

Example	Type	Explanation
Login as root	Command prompt	This means you should type in the command, "root" (without the command quotation marks), then press and release the "Enter" key. Unless otherwise noted, commands that are typed in must be followed by pressing the "Enter" key.
Press Enter or Press <Enter>		This means you should press and release the "Enter" key on the keyboard.
Press <a>		This means you should press the "A" key on the keyboard in lowercase.
Press Alt+C or Press <Alt> <C>		This means you should simultaneously press the "Alt" key and the "C" key on the keyboard, then release them both. Do NOT press the "+" key; the "+" symbol only shows that both keys should be pressed at the same time.

Use of numbered lists in this document

This document will use numbered lists when there is a need to describe procedural steps, list numbered features or concepts, and/or prioritized listed items.

Use of bulleted lists in this document

This document will use bulleted lists to convey informational data-points or concepts where no priority or process steps are necessarily involved.

Chapter 1 Introduction

1.1 Overview

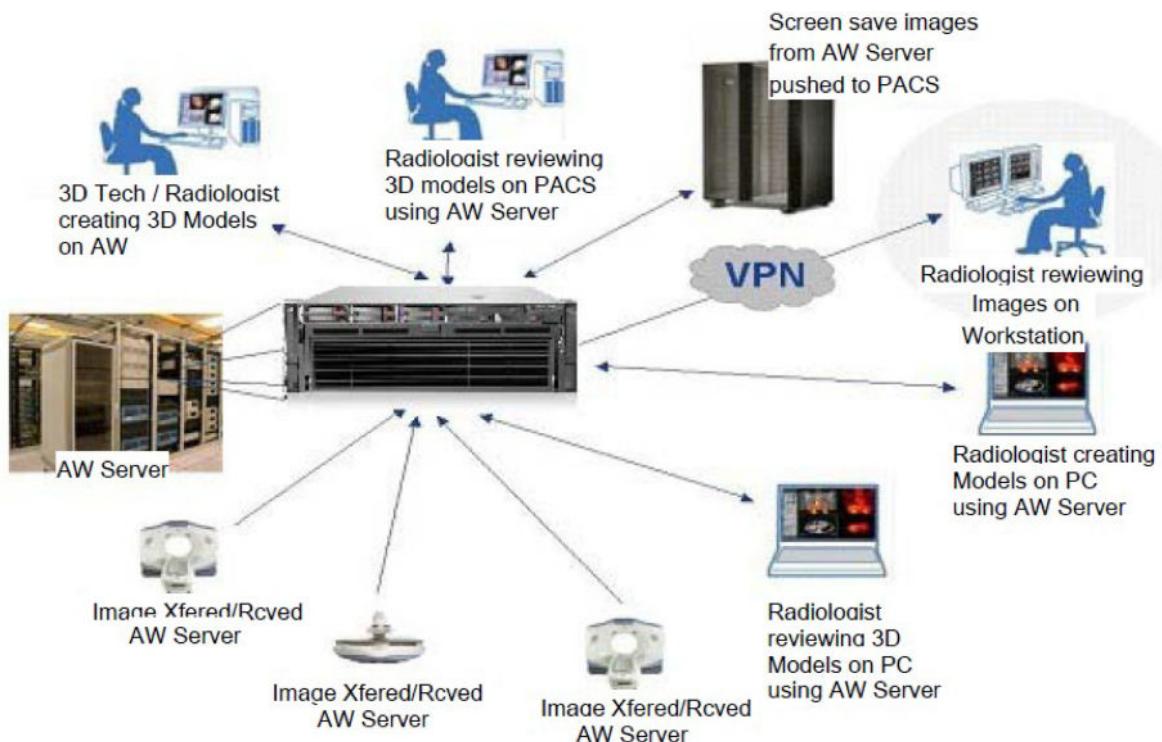
This chapter covers the following items:

- Section [1.2 Overview of an AW Server](#) on page 26
- Section [1.3 Security](#) on page 40
- Section [1.4 Service Model and Break-Fix Processes](#) on page 46
- Section [1.5 AW Server System Power-Up Sequence](#) on page 48
- Section [1.6 Site Pre-installation Specifications](#) on page 50

1.2 Overview of an AW Server

AW Server “System” Pictorial

Figure 1-1 AW SERVER - THE “USER” EXPERIENCE



AW Server - Product Description

AW Server 3.2 provides tools for processing and filming of multimodality DICOM images in a networked environment. The client and server software are designed for use with off the shelf hardware technology that meets a defined minimum specifications. If installed on a customer-owned virtualization platform (hypervisor), this must also satisfy the minimum performance 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.

NOTICE

The device is not intended for diagnosis of mammography images under any circumstances. For other images, it is the user's responsibility to ensure that monitor quality, ambient light conditions and image compression ratios are consistent with clinical application.

AW Server is a software product providing easy selection (through integration or Browser when available), review, and processing of multiple modality DICOM images from a variety of PC client machines, using LAN or WAN networks. It also allows user-selectable lossless and lossy compression schemes that are used in order to make a trade-off between speed and quality.

AW Server is intended to be used in a manner similar to the GE Medical Systems Advantage 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.

Versions of the AW Server are available with suitable hardware platforms, either rack-mounted or free-standing (tower):

- Rack-mount High Tier versions support from 16.000 to 160.000 slices and are based on:
 - the HPE ProLiant DL360 Gen10 Server (High Tier)
 - the HPE ProLiant DL360 Gen9 Server (High Tier)
 - the HPE ProLiant DL560 Gen8 Server and HP D2600 DAS or HP D3600 DAS disks array
 - the HPE ProLiant DL580 G7 Server and HP D2600 DAS disks array
- Rack-mount Low Tier version support from 8.000 slices to 40.000 slices and is based on:
 - the HPE ProLiant DL360 Gen10 Server (Low Tier)
 - the HPE ProLiant DL360 Gen9 Server (Low Tier)

NOTE

It was previously possible to insert the HPE ProLiant ML350p Gen8 Server in a rack using the Rack kit option, however this option is now discontinued.

- Tower Low Tier versions support from 8.000 slices to 40.000 slices and are based on:
 - the HPE ProLiant ML350p Gen8 Server
 - the HP ProLiant ML350 G6 Server

A "software only" version of AW Server is also available, for installation on a customer-owned virtualization platform (hypervisor). Refer to the AW Server 3.2 Pre-Installation Manual for details of Virtual Machine specifications.

NOTICE

Sun Fire™ x4450 server with **J4200 DAS** disks array **is not supported anymore** in AW Server 3.2.

NOTICE

Physical High Tier HPE ProLiant DL560 Gen8 Server and HPE ProLiant DL580 G7 Server (no DAS) are no longer supported in Seamless integration with the Universal Viewer.

The AW Server System:

The three basic components in the AW Server “system” are:

- The **AW SERVER**
- The **NETWORK**
- The **CLIENTS**

1. The **AW SERVER** component has the most diagnostic tests associated with it. **The AW SERVER is the foundation for the AW Server system, and is the direct responsibility of GEHC.**
2. Service information for the **NETWORK** includes basic connectivity testing, with links to informational possibilities if various issues arise. **The NETWORK is NOT the direct responsibility of GEHC.**
3. The **CLIENT** tests are essentially the AW Server “SYSTEM” tests. This manual provides configuration suggestions, and informational links on possible issues that could arise, as well as normal configuration setup suggestions. **Client hardware is NOT the direct responsibility of GEHC.**

It is not possible to cover ALL the potential issues that can arise with the AW Server. However, this document should be a good launching point for AW Server support in the field.

Disclaimer - Scope of this Manual

This manual is not intended to provide installation instructions. Comprehensive information for pre-requisites, installation and configuration are provided in the:

- AW Server 3.2 Installation and Service Manual,
- AW Server 3.2 Hardware Installation Manual,
- AW Server 3.2 Pre-Installation Manual.

This AW Server 3.2 Advanced Service Manual makes cross-references to these documents where relevant. For more detailed references, see [AW Server 3.2 documentation on page 22](#).

1.2.1 Product Features

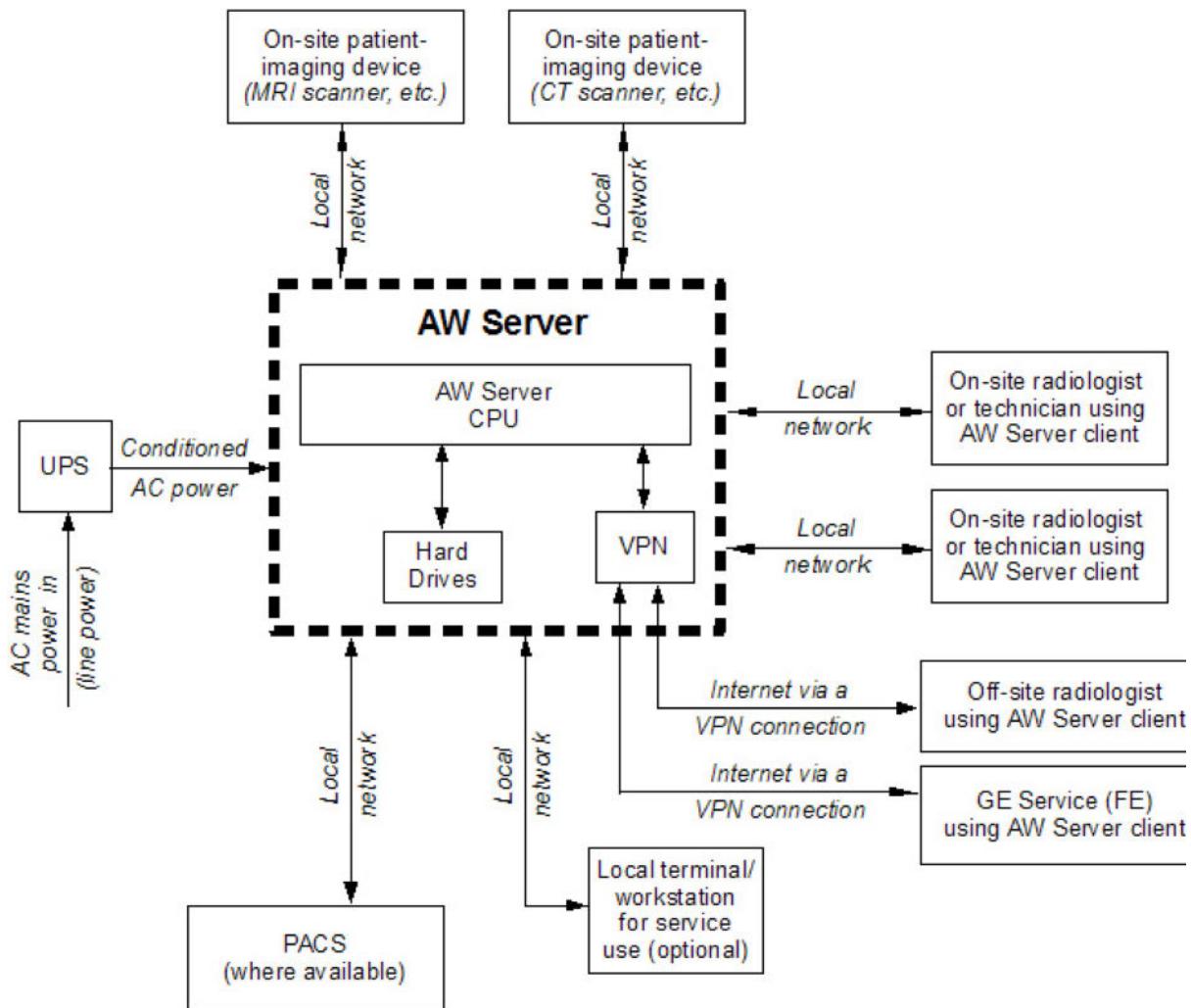
The following is a non-exhaustive list of key features and capabilities of the AW Server product:

- Web-based remote administration for authenticated administrative users, with ability to perform diagnostics, configuration, usage stats, audit trails, license usage status, and log viewing from any connected PC.
- Remote connectivity from OLC, to monitor and service the AW server, provides the same access, functionality, and security as if the user were connected to the AW Server's local network.
- Compatible with Volume Viewer applications - (example list: Volume Viewer, Volume Viewer PET, OncoQuant, Integrated Registration, Autobone, AutoLaunch) at interactive speeds sufficient for remote post processing and diagnostic review. (Note that the VV Apps software is not integrated in the platform in this release.)
- Ability to save user's preferences (for application layouts and general UI) on the server so that the same user preferences take effect on any client PC / laptop on which the user logs in.
- Server support for the concurrent licensing model for applications is available on the server. The licenses are capable of being shared with local AW's that are Floating License enabled.
- User authentication using Microsoft® Windows® Active Directory Server and eDirectory. Local account authentication and authorization package are available for the server as an option in case the facility does not use a directory server. In case of seamless integration, user authentication is supported through integration with Universal Viewer.

- Restricted patient data access based on DICOM Study Information, with the ability to assign appropriate permissions when necessary. More than one user may be assigned permission to view a given study.
- **Adjustable compression** / performance settings for optimal bandwidth usage and image quality.
- Ability for all screen content on the client to scale from a resolution of 1024 X 768 to 2MP without loss of readability of images and annotations.
- Supports dual color monitors for analysis mode.
- Ability to copy / paste images between GEHC applications and native PC applications and save batches of images as JPG's on local client PC.
- **Supported client platforms:** From Ext 4.0, only Windows®10 (32/64 bit) is supported. Previous versions support Windows® 7 SP1 (32/64 bit), Windows® 8.1 (32/64 bit) and Windows®10 (32/64 bit). With display resolution of primary monitor set to 1024 x 768 or higher. Both portrait and landscape configurations are supported.
- Dual monitors
- Integrated exam cache disk / storage on the server.
- Support for the following modalities: CT, PET, MR, X-ray, NM and Mammography (no diagnosis). Minimum modalities supported for remote 2D/3D review and advanced applications are: CT, PET and MR.
- A configurable anonymization tool is accessible from browser as well as from the filer.
- A mini-filer is available for generating output such as screen captures and exporting DICOM to JPEG's or MPEG's. (Not available in Seamless and DICOM Direct Connect modes).
- Ability to create scalable clusters of AW Servers (according to purchase options) providing stable performance for larger numbers of concurrent users.
- Support of seamless integration with Universal Viewer.
- GE Remote Update limited to upload of configuration file (no automatic upload of applications or platforms)

The figure hereafter shows a block diagram of a generic AW Server system and related options.

The main difference is only in the number of users the system will support.

Figure 1-2 AW SERVER SYSTEM - FUNCTIONAL BLOCK DIAGRAM

1.2.2 Upper-Level Functional Description

1.2.2.1 Device Description

AW Server is a software package optionally combined with off-the-shelf server-class hardware. It allows easy selection, review, and processing of multiple modality DICOM images from a variety of PC client machines using LAN or WAN networks. It allows user-selectable lossy and lossless compressions for transferring medical images.

AW Server is intended to be used in a manner similar to the current GE Healthcare AW Workstation product or as a viewer integrated in the GE PACS workflow. It is intended for creating and reviewing diagnostic evidence related to radiology procedures in general purpose radiology, oncology, and cardiology clinical areas, as well as neurology.

AW Server acts as a collaborative workflow connection between clinicians within the department and between the department and referring physicians. A server is a central repository for a diagnostic imaging exam in progress, allowing one clinician to collaborate with others via an exam referral list. From any PC, a clinician can use AW Server to export diagnostic images into other desktop applications. Interactive workflows include user interaction with applications either selected in the work-list, 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.**

1.2.2.2 AW Server terminology

THREE major terms are used to describe the AW Server "system" components:

1. **The server:**

This is the hardware, the software applications (supplied by GE), and the exam data stored by users. These can be used simultaneously by multiple people from multiple locations.

2. **The client:** This is the PC hardware an individual uses to use the applications and access and modify the patient exam data on the server. The client is typically a personal computer or laptop, and can be located basically anywhere in the world where there is a broadband network connection to access the server.

3. **The network:** The data connectivity infrastructure that the server and the client are connected to, which allows communications between the server and the client.

1.2.2.3 Virtualization and AW Server

A Virtual Machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system. A Virtual Machine (also noted "VM") can only be installed on top of a host called a "hypervisor". A hypervisor is a computer using virtualization technology to provide hardware resources (CPU, memory, storage, network) to the Virtual Machines. The main benefits of virtualization are:

- **server consolidation:** Several Virtual Machines with different guest operating system can run on a single Hardware
- **hardware independence:** the hypervisor is replacing access to hardware resources by access to abstract computing resources. Virtual Machines do not need specific drivers for each physical hardware as this is managed by the hypervisor. This means that an AW Server Virtual Machine can be installed on any hardware with enough resources in theory.
- **Isolation:** Virtual Machines running on the same hardware are isolated as if they were separate computers.
- Refer to the AW Server 3.2 Pre-Installation Manual, Requirements for Virtual AW Server to know the virtualization platforms (hypervisors) supported by the AW server.

1.2.3 Network Functional Overview

1.2.3.1 Computer Network Overview

Since the AW Server is basically a network-based "appliance" the operation of the customer's network is crucial to performance of the AW Server system. Note that the customer, and not GE Healthcare, is responsible for administering and maintaining the network.

A detailed description of computer networks is beyond the scope of this manual, but the following is a brief overview.

1.2.3.2 Purpose of the Network

In the case of the AW Server, the main purpose of the network (from our perspective) is to allow the AW Server to communicate with the customer's client computers and diagnostic imaging devices (CT scanners, MR scanners, etc.), and also with a PACS, allowing users to view, modify, and store patient images and other data. AW Server can also directly access images on PACS if integration has been configured accordingly.

1.2.3.3 Network Components

The main components of computer networks are typically routers, hubs, bridges, and switches, which work together to determine where data is sent. These devices, along with the servers and clients, are typically interconnected with either metal-conductor cables (such as twisted-pair cable) or fiber-optic cables. Wireless (RF) communication can also be used.

1.2.3.4 LAN vs WAN

The LAN (local area network) is the "local" network, contained within a facility such as a hospital or clinic. The AW Server is on the LAN, as are the users (clients) within the facility. Users outside the facility must use a WAN (wide area network), typically the Internet, to communicate with computers on the LAN.

NOTE

Unless otherwise specified, when this document refers to a network, it means the customer's local area network or LAN.

1.2.3.5 Factors in Network Performance

The two factors that are most critical to network performance of an AW Server system are bandwidth and latency. It is important that both of these measurements be within acceptable limits. If there are problems with either bandwidth or latency, the AW Server can seem slow and unresponsive to the users.

Bandwidth (capacity vs use)

Bandwidth can be defined as the maximum data transfer rate of a network, in other words, how much data the network can carry in a given amount of time. The bandwidth is the most important factor in determining the speed of a network.

Network capacity must exceed user requirements, otherwise users will experience slow transfer of data, possibly perceived as "slow computer" when it is actually neither the client PC nor the AW Server, but rather the network itself that is causing the slow response. A 1 Gb/s (Gigabit Ethernet) LAN capacity is recommended for optimum performance of the AW Server and its clients. A network speed of 100 Mb/s will give somewhat slower performance, but the performance will still be acceptable to most users. However, no matter how fast the network, users will experience slowdowns if user demands exceed network capacity.

For users outside the LAN, connection speed will usually be far slower, typically in the range of 3 to 5 Mb/s. The user will experience significantly slower client communication with the AW Server at these speeds as compared to a client connected within the LAN.

Latency

Latency is a measurement of how long it takes a packet of data to go from one point on the network to another. If latency is too long, the customer will perceive the AW Server as being slow. Latency for AW Server users outside the LAN will usually be significantly longer than within the LAN.

1.2.3.6 Network Security

A network must be secured against unauthorized users who might try to steal confidential data and/or cause malicious damage. In the case of the AW Server, protection of patient data is particularly important. Like other aspects of the network, security is the responsibility of the customer.

1.2.3.7 VPN Information

NOTICE

Use of a non-accepted VPN protocol (i.e., other than IPSec) can cause degradation of patient image quality, and possible performance issues.

WAN connectivity requires using a VPN with IPSec; Internet connection without an IPSec VPN is not supported. Please refer to the product data sheet.

1.2.3.8 Default Network Names

Note that the OS template provided with the platform gives the following default names to the virtual networks to be used:

- VM Hospital Network
- VM Private AWSERVER Network

It is possible to leave these names, but it is recommended to rename them when there is more than one AW Server on the network, to facilitate identification.

1.2.4 Client PC Performance

A client PC that is not powerful enough will make the AW Server system seem slow and unresponsive to the user, when in fact the problem is actually with the client PC. Critical specifications of the client computers include CPU type and speed, RAM, hard drive speed and free space, etc. Any "weak link in the chain" will cause the client PC to be too slow for satisfactory operation with the AW Server.

All the customer's client PCs, including those which are privately owned by users of the AW Server system (for example, a radiologist's home computer used to remotely access the AW Server), must meet the minimum specified performance requirements. Ensuring the performance of all client PCs is the responsibility of the customer. Note that this responsibility also includes the privately-owned PCs.

GE Healthcare is not responsible for client PC performance.

The client is the responsibility of the customer.

1.2.5 Remote Service vs. On-Site Service

Travel to a customer site should NOT automatically be the first choice for a repair. It is often faster and less costly to troubleshoot a customer's AW Server problems via remote access, instead of making a service call to the customer's site. This saves both travel time and on-site costs. Whenever practical, use remote access to solve customer problems.

1.2.6 Server Standalone Test - Rationale

For the AW Server 3.2 release, the server standalone test provides a link to the Service Tools HealthPage. Use this to evaluate the status of the system hardware and software sub-systems.

For details of other diagnostic tools and techniques, refer to Chapter 3.

1.2.7 Service Tools HealthPage

The HealthPage evaluates the server's configuration, hardware, and software sub-systems. The HealthPage for a virtual AW Server installation also has minor differences.

The HealthPage has several sections:

- Hardware Subsystem / Virtual Machine (and related **Sensor status details** in a separate window)
- **System Configuration**
- **Version Information**
- **Configuration and Status** (data hidden by default)
- **Software Subsystem**
- **Software Subsystem essential for Service Tools**
- **Remote Service**

The right-hand columns on the HealthPage show color-coded status information indicated by a **GREEN**, **YELLOW** or **RED** background.

- **Green** means that the status or value of that item is OK.
- **Yellow** indicates a status "Not critical" or "Not applicable"
- **Red** indicates a status "Failed".
- **White** background indicates that "status" is not applicable for that item.

Any item with red background indicates a failure, which must be investigated and fixed.

There is also a "Configuration and Status" listing that displays in a separate pop-up window on demand.

The *Configuration and Status* window does not use the green/red indicators.

- The **Hardware Subsystem** has a button to display ALL the hardware sensor details: **Sensor Details**. Click this to list **ALL hardware sensor data** with the raw values, limits, and status for specific and individual hardware identification.
- The **System Configuration** section lists basic server parameters. The following illustration example shows typical values for an AW Server installed on a hypervisor. A failure indication here means that the corresponding hardware is degraded, **has failed, is not appropriately configured or is not compliant with specifications**.

Figure 1-3 HEALTHPAGE EXAMPLE

The screenshot displays the AW Server Healthpage with several sections highlighted by red arrows:

- Virtual Machine / Hardware Subsystems:** Points to the top section containing a table with rows for CPU, Memory (RAM), Network Interface Controller, and Storage, all marked as OK.
- System Configuration:** Points to the middle-left section containing a table with various system parameters like System ID, Platform version, Hostname / IP Address, and CPU details.
- Version Information:** Points to the middle-right section containing a table with AWS build date, AWS version, EA3, EAT, Nuevo, CoLA, Service Tools, and other service details.
- Configuration and status:** Points to the bottom-left section containing a table with software subsystems like Image Management Subsystem, Firewall, Audit Server, etc., all marked as OK.
- Software Subsystem:** Points to the bottom-middle section containing a table with essential services for Service Tools like httpd, tomcat, rmiregistry, servicemli, and awsservicemli, all marked as OK.
- Software Subsystem essential for Service Tools:** Points to the bottom-middle section containing a table with essential services for Service Tools like httpd, tomcat, rmiregistry, servicemli, and awsservicemli, all marked as OK.
- Remote Service:** Points to the bottom-right section containing a table with RSvP Status (Connected and CRM verified), RSvP Connection Time (Mon 14 Jun 2021 07:51:05 AM CEST), IRIS Status (Running), IRIS Last Execution (Tue 15 Jun 2021 03:11:30 AM CEST), and IRIS Next Execution (Wed 16 Jun 2021 03:11:30 AM CEST).

- **Configuration and status.** Click the **Display** button to display data in a pop-up window:

```

Date: Fri Feb 22 08:51:22 CET 2019
=====
SITE IDENTIFICATION
-----
Hospital name : TESTbuclab
System ID : AWBUCLAB237
Country Code : --
Global Order Number : TEST123456
S/N : VMware-56 4d 4b e2 c0 f6 9d 55-6f 24
e9 6c 4d c3 e4 aa

=====
STATION CONFIGURATION
-----
Internet address : eth0 3.249.70.237
Netmask : 255.255.254.0
Default gateway : 3.249.71.250
hostname : bucaw70-237
DICOM Hostname : bucaw70-237
DICOM AETitle : bucaw70-237
DICOM Port Number : 4006
CPU : Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Nr of processors : 8
Processor clock : 2.70GHz
Operating System : HELIOS release 6.10 (Carbon)
OS Version : 6.10
Uptime : 17 days
Memory Total / Free : 64427 (MB) / 60081 (MB)
OS Disk Space Total/Free : 41 (GB) / 25 (GB)
Image Disk Space Total/Free : 94 (GB) / 76 (GB)
Backup Disk Space Total/Free : 3 (GB) / 3 (GB)
Log Disk Space Total/Free : 9 (GB) / 9 (GB)
Network Queue Status : In progress: 0 Pending: 0 Paused: 0
Failed: 0
Mount count curr./max (im. p.) : 4/36
Next fsck date (im. part.) : Sat Jul 20 19:10:49 2019
Certificate expiration date : Sat 20 Jan 2024 06:11:20 PM CET
Clam AV status : Not activated, 0
Machine type : VMware Virtual Platform ESXi 6.0
DAS serial number : Not applicable
Platform version : aws-3.2-3.2-1902.5-975c1d6d
Modality OS version [20181115] : AWS3.2_OS_5.0-1846.4-249f4bf8
UDT : (01)00840682102384 (10)AWS3D2E003D2

```

Hide

Use the scroll bar to view the entire file. Click the **Hide** button to close the window. You can also download this data by clicking the **Pull from system** button.

NOTE

The Serial Number for Virtual Machine displayed in configuration as "S/N" is attributed by the hypervisor and is similar to the following form: VMware-53 2f 21 6b 4f b8 90 5b-d4 35 05 05 18 6e 41 fb (for VMware hypervisor). For physical AW Server, the Serial Number comes from the BIOS settings.

- The **Software Subsystem** details can be investigated by analyzing the corresponding error logs in the Diagnostic - Log Viewer tool selection.

NOTE

The software subsystem service names have parenthetical references after them. These parenthetical references also appear after the log names in the log viewer — so you can select the log or logs that will contain information about that particular software subsystem service.

The Software Subsystem table also has a **Restart** button.

NOTICE

The Restart tool should be used carefully, since it restarts services used by the Clients, so temporarily disables access to the server for the users.

NOTICE

The AW Server's configuration must be registered each time it is modified by a change to the installed software. Refer to Chapter 5, [5.3.8 Registration on page 429](#).

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

The **Restart** button is like rebooting the platform software system. It shuts down the AW Server software subsystem in an orderly way, and restarts in a controlled sequence.

The Restart button is technically not part of the standalone tests. It is used for **troubleshooting a failure** in the standalone test, and only when all users are warned, or when no users are connected.

Any **RED** indicators in the **Hardware Subsystem Status** table warn of a server hardware standalone test failure. Click the **Sensor Details** button to see the details.

- Certain hardware failures such as fans that are in the process of failing, disk drives that have failed in the RAID, and correctable memory errors, might not cause the server to be down.
- Any hardware failure is a standalone failure that requires investigation and resolution by the hardware vendor. The hardware vendor dispatch process must be engaged through the GEHC Online Center. **It is important to catch all failures before they cause the server to go down!**
- Obviously, if the system is not functioning, or has any issues that cause a request for service, and the HealthPage is accessible — any hardware sensor failure should be treated as the likely cause of the system failure(s), and dispatched to the vendor for resolution before any further troubleshooting is done.

Any **RED** indicators in the **Software Subsystems Status** table warn of a failure in the server software subsystem standalone test. Some of these failures are not fatal to the functionality of the server. The Client Exporting subsystem, the Firewall, Secure Direct Connect, and the Printing Service will probably not cause the server to be down. **But these failures still must be resolved due to their potential impact on the client side.**

See Chapter 3, [3.4.1 Understanding the HealthPage on page 154](#) Understanding the HealthPage for further details.

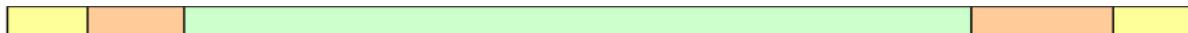
1.2.8 Network Performance

A network Performance test tool is provided with AW Server 3.2. You can also refer to Chapter 3, [3.4.5.7 Network Performance Measurement Tool \(command line tool\) on page 194](#) for details of the **neta.bat** script and related logfiles.

The AW server provides a measurement of the performance over the network. It is meant to show you how fast this application will run on this PC over this network. The network test sends data over the network same way the AW Server application does. The test results (Mb/s) reflects not only the bandwidth but also the latency of the network.

The bandwidth measurement provided is not fully a measurement of the customer's network bandwidth. Instead, it is a measurement of the file transfer bandwidth available between the client and the server at this moment. Please note that this tool never fully loads the customer's network.

The time measured includes the following:



Open file on server	Compress file	Transfer file from server to client	Uncompress file on client	Save file on client
---------------------	---------------	-------------------------------------	---------------------------	---------------------

The above pictorial represents the basic workflow of the preview pane and results viewer in the AW Server end-user-browser-application.

We can conclude that the network bandwidth of our tool will be affected by:

- The customer's network speed (including the speed of all routers and switches between the server and client)
- The current usage of the customer network. (i.e. if a CT scanner is currently transferring images from an exam to a PACS, the network will be loaded, and performance slower).
- The network card speed on the client PC
- The CPU speed of the client PC
- The disk speed of the client PC
- Memory (RAM) speed of the client PC
- The amount of RAM available on the client PC.

The performance of our application may be improved by improving any of the above. However, upgrading to a faster client PC when running on a very slow network may be of minimal help if the bottleneck is the network itself.

On a gigabit (GbE, or 1 Gb/s) network, it will usually be faster to run with browser/preview (lossless) compression **OFF** and application compression **OFF** - because it takes the client PC longer to uncompress the image than the time saved transferring the image over the fast network. However, running the client checker network test with compression on and off will tell you which setting works best on this PC. The browser/preview compression setting is under the TOOLS menu.

So, it will not be unusual for our tool to be able to achieve **25MBps** transfer rates on a gigabyte network with compression off, but only **8MBps** transfer rate with compression on. On 100BASE-T networks, compression will almost always be faster, unless the client PC is very old and slow.

Compression on

Open file on server	Compress file	Transfer file from server to client	Uncompress file on client	Save file on client
---------------------	---------------	-------------------------------------	---------------------------	---------------------

Compression off

Open file on server	Transfer file from server to client	Save file on client
---------------------	-------------------------------------	---------------------

In this case, it will be faster to run with compression off.

The speed of our tool will be similar to the speed an FTP file transfer can achieve — such as the download of the client application from the server to the client.

Here are some sample bandwidth rates that can be returned from the client checker's network tool, and the type of corresponding performance the customer will see when using our applications:

Client location	Measured rate	Performance
Inside the hospital, with a GB network	25MBps	Excellent
Inside the hospital, with a 100BASE-T network	8MBps	Very good
Inside the hospital on a wireless network	1.5MBps	Good
From home	200KBps	Poor
From home	50KBps	Unusable

1.2.9 Maintenance Mode

There are a number of service tool interventions that can either cause the server to be unavailable — by temporarily disconnecting clients — or can potentially cause file loss or corruption if user files are being accessed when the intervention is performed. Maintenance Mode has been designed to minimize the risk of these problems.

NOTE

Maintenance Mode provides a way to safely perform various important maintenance and service functions without "unexpectedly" disconnecting clients or corrupting user files. It is a combination of tool design and process design, and needs to be used within the context of the needed service intervention. It is NOT a one-size-fits-all or one-button-and-done tool

For tasks that require that all clients be disconnected, the Maintenance Mode tool allows the service user to perform these tasks safely by disconnecting clients in a planned and controlled way. The service user can broadcast messages to all clients to warn their users of an impending disconnection and shutdown. This allows time for users on all clients to save their work and close all files, thus preventing data loss or corruption.

NOTE

Users will not be able to connect to the AW Server as long as it is placed in "Maintenance mode".

1.2.10 Groups, Roles and Members

There are four built-in "local" accounts, each with an assigned role that corresponds to the account name:

- **service** account = GE Service role (ALL Service Tools access)
- **admin** account = Administrator role (Almost ALL Service Tools access)
- **standard** account = Standard User role (Few Service Tools access)
- **limited** account = Limited User role (No service tool access)

The **Groups** tab is located under **Administrative > Configuration > Users (EA3)**.

In order for a new user (local or enterprise) to have proper access to the server applications and/or tools, the user must be assigned a role - which by definition determines their access privileges. The way to do this is to add the new user or the new enterprise user's group to the existing built-in roles (GE Service, Administrator, Standard User, Limited User).

NOTE

When AW Server is configured in Full or Seamless integration, Service and Admin users are authenticated locally and cannot display images. There are no Limited users. All authenticated users have the Standard User Role.

See [A.5 Users, Groups, Roles and Members on page 473](#) for more details.

1.3 Security

1.3.1 Password Management

1.3.1.1 Default Passwords

This section provides the account “DEFAULT” passwords that come with the native hardware and software. These passwords should be changed during the installation procedure in order to increase security.

This applies to both the Linux OS passwords and the AW Server users passwords.

Default Passwords

The system default passwords for the built-in accounts are as follows:

Account Type	Account Role	Login	Password
• Service Tools • AW Server Client	Administrator	admin	Wbgttl&25
• Service Tools • AW Server Client	GE Service	service	Geiaw&08
• Service Tools* • AW Server Client	Standard User	standard	Wbgttl&25
AW Server Client	Limited User	limited	Wbgttl&25
Command prompt	GE Service	sdc	adw2 . 0
Command prompt	• GE Service • IT Admin	root	Tbd&bu
InSite	GE Service	insite	Geiaw&08
iLO	• GE Service • IT Admin	root	changeme
Universal Viewer Server		AWDakota or AWUSER	GEpac#123
Crypto Officer			Tbd&bu2020

NOTICE

Keep these passwords for the built-in accounts for GEHC knowledge and use only. Setup the Admin account above with its own dedicated password. If there are site IT Admin rules that require knowledge of the built-in account information, and perhaps require the passwords to be changed – this should be complied with as long as the service center or online center process for documenting these changes is adhered to. There should NEVER be a case where the OLC cannot access the tools because a built-in account change was not communicated.

1.3.1.2 Changing Passwords

The default passwords that come with the native hardware and software shall be changed during the installation procedure in order to increase security.

This applies to both the Linux OS passwords and the AW Server users passwords.

The AW Server users passwords shall be changed as well, in case they have expired (default passwords lifetime is 60 days (in RMF mode) or 90 days in other modes).

Refer to section [A.6 Password Change on page 484](#).

1.3.2 AW Server Extra Security Layer Login

The AW Server Client Login interface provides the option to select a higher level of login security. When the box is checked the HTTP communication is done via **HTTPS - Hypertext Transfer Protocol over Secure Socket Layer** or **HTTPS**.

Protocol over Secure Socket Layer or **HTTPS**. This is a URL scheme used to indicate a secure **HTTP connection**. It is syntactically identical to the http:// scheme normally used for accessing resources using HTTP. Using an https: URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP. This system was designed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for **security-sensitive communication** such as payment transactions and corporate logons.

HTTPS is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks.

An https: URL may specify a TCP port; if it does not, the connection uses port 443 (unsecured HTTP typically uses port 80).

Organizations may also run their own certificate authority, particularly if they are responsible for setting up browsers to access their own sites (for example, sites on a company intranet), as they can trivially add their own signing certificate to those shipped with the browser.

For the purposes of AW Server operation, it is recommended to use this option when logging in from a remote network or VPN connection.

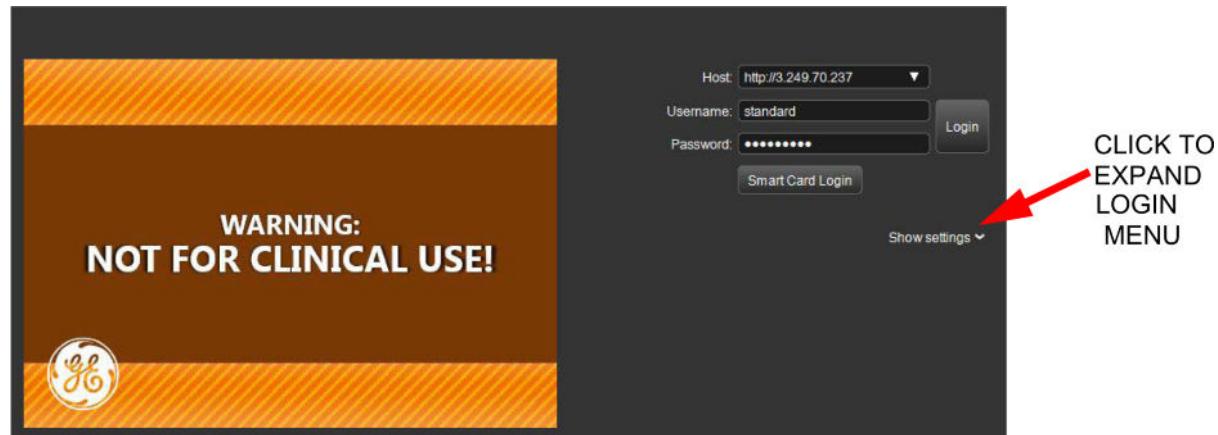
If unable to connect to the AW Server or start applications when running from outside the local network through a VPN, it might be because the VPN or site security policy is rejecting server network traffic for security reasons. This can be fixed by turning on the AW Server's security layer below.

Or, the site VPN solution is not compatible with AW Server functionality — see Network Functional Overview.

NOTE

Secure mode is “off” by default. Adding this security layer will slow down the performance somewhat.

Figure 1-4 EXTRA SECURITY LAYER LOGIN (AWS CLIENT LOGIN)



NOTICE

For seamless integration, secure communications for clients via HTTPS can be configured using the Universal Viewer Site Configuration Tool. See the Universal Viewer Site Configuration Tool Service Manual.

1.3.3 Patient Confidentiality Notice

NOTICE

Informational NOTE regarding patient confidentiality in the event of an uncontrolled **CLIENT PC CRASH**.

The preview pane and results viewer store patient images on the CLIENT PC as they run.

Normally, when the application exits or crashes, those images are deleted. However, if "Windows" crashes or the CLIENT PC loses power, the AW Server client application isn't able to clean up those images, and some images containing confidential patient data may be left in the temp directory of the CLIENT PC.

To delete these images after this type of crash, either start the AW Server application again on the client which will automatically re-use and clear the temp directory — or manually go to:

- C:\Documents and Settings\<username>\Local Settings\Temp\rmimages
- **DELETE all contents** in this directory.

Automatic deletion of files at start up:

If the customer would like to have the files deleted automatically every time Windows starts up, then **move the shortcut as follows**:

Move the file named "Delete Temp Files.exe" >>> from directory: c:\Program Files\aws*** >>> to directory >>> c:\Documents and Settings\All Users\Start Menu.

1.3.4 Removal of Image Data

In order to properly delete Image Data from the AW Server hard disks, it is mandatory to use 5534806 - Disk management Tool, when available from your local Pool of Tools and follow instructions given in the 5500610-1EN - Disk Management Tool Service Manual delivered within the kit.

This tool allows to make attempt at recovering image data more difficult, thus ensuring better protection of Patient Privacy.

Also refer to Service Note **SNAW3037** available from GE Healthcare Documentation Portal, detailing the process for AW's

1.3.5 Working in an IT Center or Data Center Environment

1.3.5.1 Security Rules

The AW Server hardware is typically located in a room which is part of an IT center or data center for the facility. The IT department is responsible for data center, and the network that the AW Server connects to. It is their responsibility to keep this equipment secure and to maintain minimum performance standards. Therefore the AW Server is, to a large extent, under the control of the facility's IT department.

Know who "owns" what: GE responsibilities vs. vendor vs. customer responsibilities: see [1.4 Service Model and Break-Fix Processes on page 46](#).

1.3.5.2 Customer IT Security Policy

Building

Many hospitals and clinics require visitors such as FEs to obtain a security badge upon arrival at the facility, and may also require FEs to be supervised or accompanied while at the facility. This could be by someone from the site's IT department, or from another department such as security.

Equipment – Physical, Environmental, and Electrical

The IT department is responsible for ensuring that all IT-related systems, including the AW Server, are protected from unauthorized physical access and also from physical and electrical hazards such as mechanical damage, overheating, flooding, fire, over/under voltage conditions, etc.

Controlled electronic access – user accounts and authorizations, passwords, firewalls, etc.

The IT department is responsible for preventing unauthorized electronic access or "hacking" of equipment. This is necessary to protect the privacy of patients— data, and also to prevent possible malicious damage and/or theft of customer data.

Preventive measures can include control and configuration of firewalls, user accounts, passwords, anti-virus software, firewalls, and other means. Do not change any passwords or disable any firewall or other security software without permission. Do not log into or modify any equipment other than the AW Server without permission.

User access

In addition to preventing unauthorized people from accessing IT equipment, the IT department also needs to ensure that authorized users have access to software and accounts. This requires that IT maintains current, centralized records of all user accounts and passwords. Always notify the IT department before you modify any user account names or passwords for the AW Server.

Control of outages.

All routine maintenance and upgrades must be scheduled and approved via IT. Unscheduled rebooting of equipment can cause service outages of other equipment. IT departments typically have service-level agreements with the site's functional areas (e.g., with each department in a hospital). These agreements require the IT department to maintain a certain level of security and functionality for the IT equipment that these departments rely on. Note that COLA services are not available during outage/reboot.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

NOTICE

AW Server is not a storage device thus GE does not make any related claims about potential data loss.

NOTE

In the event of an equipment failure, contact the IT department as soon as possible to coordinate your troubleshooting and repair activities. THIS INCLUDES ACCESSING THE AW SERVER REMOTELY.

Data backup and restoration.

IT departments perform regular backups of data. When data is lost or corrupted, they restore the data from backup files.

1.3.5.3 Physical Security

NOTICE

Your actions may have unwanted consequences that can cause service outages or other major problems for other equipment or even other departments. Plan carefully before making any changes, and coordinate your actions with the IT department before you start working on the AW Server.

- Be cautious; think before changing anything that could cause problems. For example, ask permission from IT before changing network settings, because doing so could affect something seemingly unrelated, such as a PACS, etc.
- Don't disconnect or power down any equipment without permission. This includes turning off circuit breakers that supply power to the AW Server. This also applies to disconnecting or changing any data cables, power cables, etc.
- Keep doors and equipment closets/cabinets locked except when you require access. Be sure to secure the site when you leave.
- Avoid creating any potential hazards — fire, electrical, chemical, mechanical, etc.

1.3.5.4 System Security

NOTICE

Default passwords are a security risk; all default passwords should be changed to unique, complex passwords as soon as possible. Note that if you change the service account password, you must advise the OLC.

NOTICE

Turning the firewall off and then forgetting to turn it back on can create a security risk by exposing equipment to unauthorized access. This also applies to other security-related software such as anti-virus, etc. Always make sure to re-enable the firewall, anti-virus, and any other security-related software when you have finished your service call.

NOTICE

It is also strongly recommended to set the system to boot from hard disk first (if not done yet), and set a Administrator password for the system BIOS. Refer to [A.22 Hardware Security on page 517](#) for instructions.

Before you leave the customer site:

- Secure all doors, equipment, closets/cabinets, etc. as they were before you arrived.
- If you have changed any settings such as passwords, user account names, configuration settings, etc, give this information in a secure manner to the IT department so they can keep track of it.
- Reactivate all security-related software that you have temporarily disabled: firewalls, anti-virus, etc.
- Ensure that ssh_enabler has been disabled - except if explicitly needed (for example, for IT on-watch monitor).
- If you have temporarily disconnected any data or power cables, reconnect them.

- Notify the IT department that you are finished, and that you are leaving. Make sure they have your contact information so they can contact you if necessary.
- If you have disabled any intrusion or motion alarms, re-enable them.
- Return any keys and/or temporary ID badges for the facility.

1.3.6 Authentication Certificate

Occasionally, customer IT policy may require a trusted third party certificate that contains the identity of the owner.

This capability is not communicated in any product documentation, however the AWS Apache web server allows installation of a trusted third party certificate.

Purchase of a trusted third party certificate is the responsibility of the customer and should be driven by the site IT Admin, or designate.

If requested by the customer, follow the process described in [A.21 Installing/renewing an AW Server external CA signed certificate on page 514](#) to install a third party certificate.

NOTE

The installation process requires a re-start of the *apache* web services and will disrupt any connected clients.

This manual does not cover the generation of a certificate file, nor the corresponding certificate file.

1.3.7 Server Firewall (PNF)

The AW Server PNF (**Product Network Filters**) software and configuration is automatically installed with the platform software load. It is automatically configured in a "**default**" configuration for the AW Server environment, and should not require any service intervention.

For this reason, it does not have a tool interface in the Service Tools web interface. For the AW Server product, PNF is only accessible via command-line.

The following information is for "information" only. Under "normal" circumstances, none of these configurations should need to be interacted with by field service.

PNF has two modes of operation: **ON** and **OFF**.

- In the **ON** state/mode, PNF will allow only the network communications that are specified by its configuration and reject all the rest.
- In the **OFF** mode, PNF will allow all communication (subject to only the filters set by the modality script).

NOTICE

THE SERVER IS EXPOSED TO A SECURITY RISK WHEN THE PNF FIREWALL IS TURNED OFF! Malicious users can login via SSH and access, corrupt, or delete sensitive files. By default ssh_enabler should be off (except if explicitly needed - for example, for IT on-watch monitor), but verify when leaving the site. The server can be used for unauthorized purposes. Vulnerability scans will fail, etc. BE SURE THE FIREWALL IS ON when you are finished working on the AW Server!

The mode can be changed using the manager Command Line Interface (CLI), and is persistent across reboots.

The folder **/usr/share/gehc_security/pnf** contains scripts and files related to pnf management.

For more detailed information, refer to Chapter 3.

1.4 Service Model and Break-Fix Processes

1.4.1 Introduction - AW Server Installation & Warranty Time Reporting

NOTE

The AW Server TOTAL installation is designed to be completed within roughly one work shift - approximately 8 to 11 hours:

1.4.1.1 Installation

Basic Installation:

- AW Server physical installation: 2 hours (DL580 / DL560 / DL360 only) 4-5 hours for DL580 / DL560 / DL360 with all equipment options, 30 min-1hour for ML350 G6 and ML350p G8
- Software installation time + configuration + 1 client installation: 4 hours

Extended Installation:

- R3000A CAT (auto) - FE installing additional clients (8 hours)
- R0906CM CAT (auto) - FE training IT admins
- When handled by GEHC IT, some professional services can be added

1.4.1.2 Installed Base In Warranty Costs (IBIW)

- The warranty cost goal for AW Server is estimated below:
- This Average labor cost is based on:
 - One service call every 6 months (or 2 times per year).
 - Each service call consisting of an Elapsed Time to Repair of 6 hours (2 hours travel to site and 4 hours MTTR per node)

1.4.1.3 Installed Base Out of Warranty Costs (IBOW)

- The Installed Base Out of Warranty Cost includes Service Contract and Hourly Billed Service/ Year is estimated from an update of the AW Server product costs:
- For AW Server High Tier, the cost of AW Server parts is not assessed if in the out of warranty model.

1.4.1.4 Periodic Maintenance

- PM procedures are not applicable for GE HC IT systems, since real-time monitoring is available for server class hardware and SNMP traps shall be defined for monitoring of selected software services.
- Currently, there are no PM schedules recommended by the hardware vendor for class hardware used in the AW Server turnkey package.

The business intent is to accurately measure product quality by having reliable service installation and warranty records and metrics.

1.4.2 Maintenance Roles

1.4.2.1 Physical AW Servers (GE-supplied)

The GEHCS FE is responsible for:

- Troubleshooting all problems with the AW Server.
- All software-related problems will be repaired by GEHC.
- Managing (not executing) server maintenance.

The equipment vendor (HP) is responsible for:

- Resolving all hardware problems for high tier AW Servers, according to the warranty / break-fix model (see below)

The customer IT Admin is responsible for:

- Server locale provision and management, consistent with the requirements stated in the AW Server 3.2 Pre-Installation Manual.
- Deploying client software (apart from the first, single site client installation)
- Maintaining the customers' own PCs (Hardware, Operating System, Displays...) and Network (Hardware & Software) connection between these PCs and the AW Server to always meet the defined minimum specifications.

NOTE

the minimum required specifications should be explained to the customer's IT department, since they are responsible for solving problems related to network and/or client performance issues.

- To identify and retain an AW Server point person at their sites who will be trained by GE to install (or reinstall or uninstall) future AW Server clients and use the GE provided troubleshooting tools to maintain the clients.
- Complete GE provided diagnostic task checklist prior to contacting GE service and send client error reports to GE Service when reporting any issues
- Maintaining DICOM nodes
- Maintaining DICOM printers
- User management (inc AD integration, group creation, etc)
- CA certificates
- Audit log repository
- Remote Connectivity. If applicable, Customer is responsible for providing and maintaining an appropriate Broadband connection at the site that GE Healthcare may use to provide remote diagnostic service for the products. Eligible products include an uptime commitment during the warranty period, provided Customer maintains a Broadband connection in accordance with GE Healthcare specifications and allows GE Healthcare to remotely monitor performance of the products via this connection. GE Healthcare will provide details of this uptime commitment for eligible products.

1.4.2.2 "Virtual AW Server" on Customer-supplied Physical Server

AW Server 3.2 is intended for installation in a hypervisor environment.

The customer IT Admin is responsible for (in addition to responsibilities defined in previous section, where applicable):

- Allocating resources on a server. These must correspond to the minimum specifications for a virtual AW Server, in term of disk space, memory available and CPU cores.

- Providing the hypervisor layer and loading the OS for AW server, from a template delivered by GEHC.

NOTE

Installation of the template may be done by a GEHCS FE under customer IT Admin responsibility.

- Managing their own Service contract with the server hardware supplier.

NOTE

AW Server software is considered "out of GE warranty" and indeed unserviceable until customer validates return to service of server with hypervisor layer prerequisites.

The GEHCS FE is responsible for:

- Loading and configuring the AW Server Platform SW, as well as installing the Advanced applications, and installing one Client.

1.4.3 Break-Fix Processes

Refer to Chapter 7 [7.3 Break-Fix Processes on page 448](#).

1.5 AW Server System Power-Up Sequence

NOTICE

The information and procedures in this section apply only to GE-supplied hardware. Do NOT use to install or maintain customer-supplied hardware on which AW Server platform software (in virtualized mode) is or will be installed; refer instead to customer site IT policies and procedures.

1.5.1 HP DL580/DL560 High Tier Server Power-Down / Power-up Sequence

For the initial physical installation of the system, the GEHC FE will perform the initial power-up, and be responsible for managing the correct sequence.

For subsequent system power-down and power-up operations, there is a specific procedure that needs to be strictly followed, or there is a risk of serious personal injury and of disk partition initialization failure(s).

1.5.1.1 Power-Down

The DL580/DL560 server can be shutdown via the software, and via the iLO service processor. But the DL580/DL560 must have both power cords removed to completely shutdown.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

1. Power down DL580/DL560 normally.
2. Remove A/C power
 - a. for a DL580 hardware – physically disconnect the four power cables.
 - b. for a DL560 hardware – physically disconnect the two power cables.

3. If the server has a DAS, remove power to the D2600 or D3600 DAS (Direct Attached Storage) chassis — two power cables

WARNING

To reduce the risk of personal injury, electric shock, or damage to the equipment, before any field maintenance to the server, always remove all attached power cords to cut power supply to the server. The front panel Power On/Standy button does NOT completely shut off system power. Portions of the power supply and some internal circuitry remain active until AC power is removed.

1.5.1.2 Power-Up

The HP D2600 DAS/HP D3600 DAS must be powered up first so that it can synchronize and attach all of its disk partitions before the DL580/DL560 accesses it.

1. Plug in A/C power to the HP D2600 DAS or HP D3600 DAS (two power cables).
2. Wait for one minute and plug in A/C power to the HPE ProLiant DL580 G7 Server (four power cables) or to the HPE ProLiant DL560 Gen8 Server (two power cables)
3. Apply power to the HPE ProLiant DL580 G7 Server/HPE ProLiant DL560 Gen8 Server with the power button on the front of the chassis.

See also in the AW Server 3.2 Hardware Installation Manual, Job Card IST004 - HP DL580 G7 server Installation Steps for HPE ProLiant DL580 G7 Server or Job Card IST003 - HPE ProLiant DL560 Gen8 Server Installation Steps (for HPE ProLiant DL560 Gen8 Server) for further details of Power-up.

1.5.2 HP DL360 Server Power-Down / Power-up Sequence

This procedure below is applicable for both the HPE ProLiant DL360 Gen10 Server and HPE ProLiant DL360 Gen9 Server Low Tier and High Tier.

No particular precaution shall be taken to start the HPE ProLiant DL360 Gen10 Server and HPE ProLiant DL360 Gen9 Server, as the image disk array is fully integrated into the server hardware.

1.5.3 HP ML350 Low Tier Server Power-Down / Power-up Sequence

This procedure below is applicable for HPE ProLiant ML350p Gen8 Server and HP ProLiant ML350 G6 Server.

No particular precaution shall be taken to start the HPE ProLiant ML350p Gen8 Server or HP ProLiant ML350 G6 Server, as the image disk array is fully integrated into the server hardware.

1.5.4 Virtual Machine Power-Down / Power-up Sequence

1.5.4.1 Power-up

In order to power on the Virtual Machine, access to the hypervisor is needed.

1.5.4.2 Power-Down

The AW Server Virtual Machine can be powered down using the Service Tools Reboot menu.

Alternatively, the IT admin can power down the VM from the hypervisor interface. This should be limited to specific case where the IT admin needs to power down the VM for hypervisor management tasks. It is required to perform a "Shutdown guest" in order to gracefully shutdown the system. Do not use the "Power Off" function.

1.5.5 Normal— OS Startup/Boot Options

EFFECTIVITY:

- After the last OS reboot, during a load-from-cold
- During normal server reboots

INFORMATION:

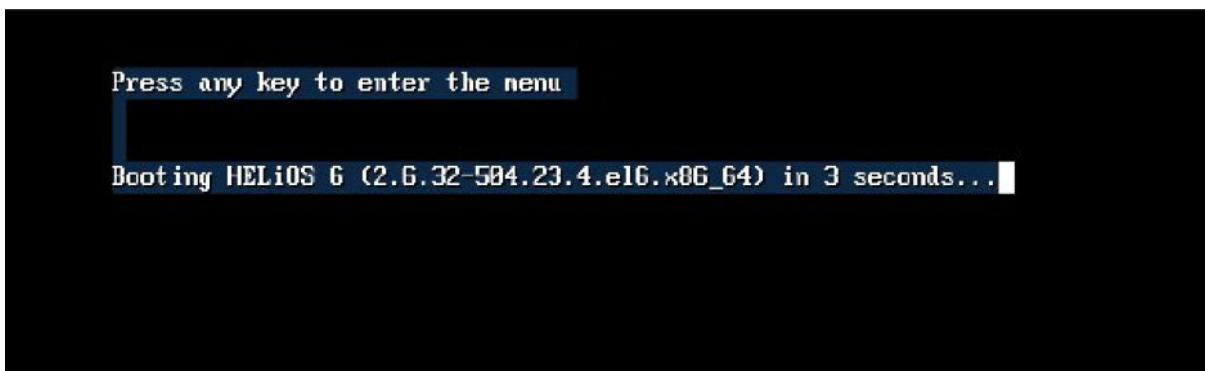
- The system will display the following or similar example “Booting HELiOS...”.

ACTION:

- **LEAVE THE DEFAULT SELECTION**, and the server will automatically continue to complete a normal boot-up from the hard disk—or—you can press the <ENTER> key with the default selection automatically high-lighted, and shown in the "example" below.
- **DO NOT CHANGE OR SELECT TO ANOTHER OPTION**

The below screen is only an example—the ongoing implementation and version numbering may be different.

Figure 1-5 BOOT OPTIONS



1.6 Site Pre-installation Specifications

Refer to the AW Server 3.2 Pre-Installation Manual, Site Pre-installation Specifications.

Chapter 2 Service Tools

2.1 Overview

This chapter covers the following items:

- Section [2.2 Service Tools Overview on page 51](#)
- Section [2.3 Initial Configuration menu on page 56](#)
- Section [2.4 Administrative Options menu on page 75](#)
- Section [2.5 Tools Menu on page 86](#)
- Section [2.6 HP iLO Service Processor on page 101](#)

2.2 Service Tools Overview

This chapter introduces the AW Server's online tools for configuration and diagnostics.

2.2.1 Service Tools Accounts

There are four built-in local Service Tool accounts, each with an assigned role that corresponds to the account name:

- admin account = Admin Role (Admin Service Tools access)
- service account = GE Service Role (All Service Tools access)
- standard account = Standard Role (Few Service Tools access)
- limited account = Limited Role (No service tool access). Does not apply in Seamless Integration mode.

The default login names and passwords for the built-in local Service Tool accounts shall be changed to unique, complex passwords at installation time (refer to [1.3.1 Password Management on page 40](#)).

NOTE

The tools available to a user are determined by the User's Role assignment (and in a few cases by the integration mode configured). The four levels of user roles are described as follows. Users who do not have service privileges will not see all the tools:

Limited User: Typically a referring physician or someone with little or no system knowledge. A limited user has access only to specific exams and applications, and NO access to Service Tools.

Standard User: 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 customer feels properly trained for this software use (radiology assistant, physician assistant, etc.).

Admin User: A person who manages the computer system within an organization. In larger organizations this could be someone in the IT department. In smaller organizations (such as standalone sites), this could be a user who has been designated as the administrator.

Service User: GE Service personnel only. Service users have access to all Service Tools.

The Service Tools login will also work for any valid enterprise account(s) that are setup on the network, and if the EA3 enterprise configuration is successfully completed.

- However, in order to make the account(s) operational, the account group information must be known in order to add the group to one of the built-in roles in the Service Tools Users (EA3). Otherwise, the server configuration will not know what permissions to assign, and the account will not work.
- The Users (EA3) tool, group assignment, and account creation is described further on in this section.

NOTE

See also the access level matrix in [2.2.2 Service Tools Access Privileges on page 52](#).

2.2.2 Service Tools Access Privileges

There are four different user-privilege levels for the AW Server: **service**, **admin**, **standard**, and **limited**.

The following matrix shows which Service Tools the four different user levels have access to.

- The GE Service Role has access to all Service Tools.
- Administrator has access to **admin** & **standard** tools.
- Standard User has access to only **standard** designated tools.
- Limited User does not have access to Service Tools.

Tool	service (GE Service)	admin (IT Admin)	standard	limited
Health-page	X	X		
Initial configuration / Remote Service	X			
Initial configuration / Device Data	X			
Initial configuration / Contact	X	X		
Initial configuration / ST Language	X			
Initial configuration / Time Settings	X	X		
Initial configuration / Database Deletion Settings	X	X		
Initial configuration / SNMP Configuration	X	X		
Initial configuration / Platform Configuration	X			
Initial configuration / Licensing	X			
Initial configuration / Scalability	X	view only		
Initial configuration / Audit Trail (EAT)	X			
Initial configuration / Prodiag	X			
Initial configuration / GIB Data	X			
Initial configuration / Hardening	X			
Administrative / Configuration / DICOM Hosts	X	X		
Administrative / Configuration / DICOM Printers	X	X		
Administrative / Configuration / PostScript Printers	X	X		
Administrative / Configuration / Users (EA3)	X	X		
Administrative / Configuration / Users (OS)	X			
Administrative / Configuration / Smart Card Configuration	X	X		
Administrative / Configuration / Client Timeout	X	X		

Tool	service (GE Service)	admin (IT Admin)	standard	limited
Administrative / Configuration / Preprocessing	X	X		
Administrative / Configuration / MailSender	X	X		
Administrative / Configuration / End Of Review	X	X		
Administrative / Configuration / Web Client	X	X		
Administrative / Configuration / XE Configurations	X	X		
Administrative / Configuration / Certificate Management	X	X		
Administrative / Utilities / Clients	X	X		
Administrative / Utilities / Network Queue	X	X	view only	
Administrative / Utilities / Print Queue	X	X		
Administrative / Utilities / Image Database	X	view/delete only		
Administrative / Utilities / Application Usage Data	X	X		
Maintenance / Maintenance	X	X		
Maintenance / Version Management	X	X		
Maintenance / Register Configuration	X	X		
Maintenance / Backup/System configuration	X	X		
Maintenance / Backup/User preferences	X	X	X	
Maintenance / Restore/System configuration	X	X		
Maintenance / Restore/User preferences	X	X		
Maintenance / Network	X	X		
Maintenance / Database Recovery	X			
Diagnostic	X			
Tools / Terminal	X			
Tools / File transfer	X			
Tools / Reboot	X	X		
Tools / Preferences/Manual Import	X	X	X	
Tools / Preferences/Share preferences	X	X	X	
Tools / Preferences/User-share assignment	X	X		
Documentation / Documentation "for standard and admin"	X	X	X	
Documentation / Documentation "for service"	X			
Documentation / Links	X			

2.2.3 Logging into Service Tools

- At the Client PC or FE laptop, open a browser (Internet Explorer®) and type in the AW Server's IP address.
- When the page loads, click on the Service and Administrative Tools **Launch** button.



The login page appears.

3. Login to Service Tools as **service**. Use the default service password.

If this password doesn't work, contact GE service or the site's IT admin to get the current password.

The *Service Tools HealthPage* appears. See [3.4.1 Understanding the HealthPage on page 154](#) for details.

Virtual Machine	Status
CPU	OK
Memory (RAM)	OK
Network Interface Controller	OK
Storage	OK

NOTE

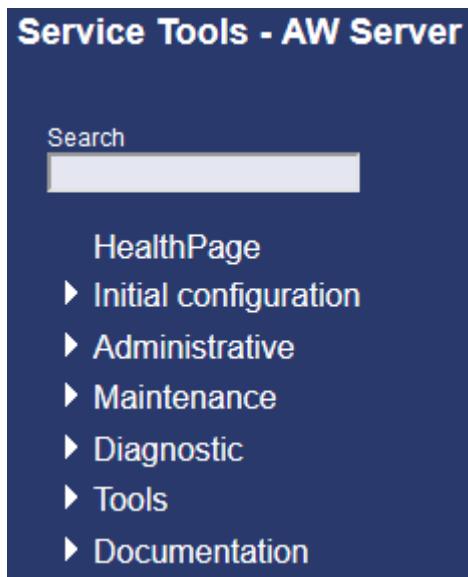
In AW Server 3.2 there is no warning message to inform that GIB data has not been sent to GE. Instead, a message appears in the banner at the top of each Service Tools page.



2.2.4 Service Tools Menu Tree

2.2.4.1 Navigating in Service Tools

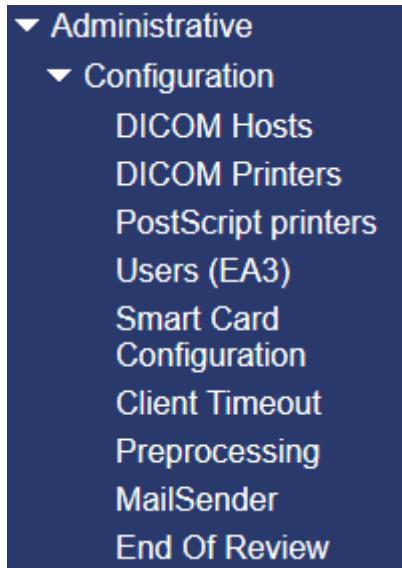
The Service Tools menu tree in the left-hand panel contains several categories of tools and options. By default, only the top level menu categories are shown, however other options are available by expanding the tree.



To expand a menu category, click any menu item that has an arrow ▶ to the left of it. The menu item will expand to list the related menu items below it. If there is no arrow, the section cannot be expanded any further. To collapse the expanded list, click the □ arrow next to the first item in the list.

When the menu expands, click the name of the tool you want to display. Note that some sections have sub-headings (i.e., additional levels) that do not display until you expand the next-lower level.

For example, in the following illustration, note that the sub-menu **Administrative > Configuration** includes items **DICOM Hosts, Users (EA3)**, etc. through **End of review**.



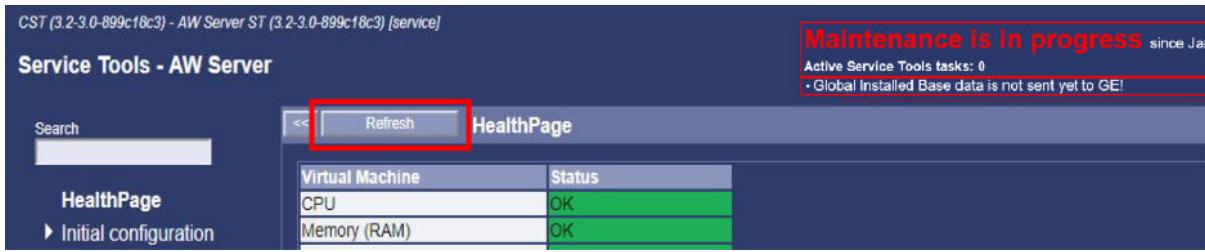
NOTE

Installation and configuration tasks (**Initial configuration** and **Administrative > Configuration**) are not fully covered in this manual. They are covered in more details in the AW Server 3.2 Installation and Service Manual.

2.2.4.2 Refreshing the Service Tools

When browsing the Service Tools menu, you might need to refresh the information on the page that you are currently displaying.

On the upper part of all tabs in the Service Tools, a "Refresh" button is available.



It allows to refresh the current tab. This is a useful replacement of the browser refresh function (F5 key), because the browser refresh brings back to home page and loses the current tab.

NOTE

Some menus also have their own *Refresh* button that only updates certain information on the corresponding page.

2.3 Initial Configuration menu

This is a menu heading for tools that are normally used only during installation or reinstallation. The menu items under Initial Configuration are described below. Refer to the AW Server 3.2 Installation and Service Manual for more details.

2.3.1 Remote Service

This is the screen that is used to configure the server for Remote Connectivity (if applicable):

- Insite connectivity (version prior to AW Server 3.2 Ext. 4.2) – Model Type: **_AWS32**
- RSvP connectivity (from version AW Server 3.2 Ext. 4.2) – Model Type: **AWS32_RSVP**

NOTICE

InSite/RSvP is not provided for AW Server 3.2 systems in EDS environment as it is not used by EDS (which uses another remote service tool).

Refer to the Installation Manual, **Job Card IST008 - Remote Service** for more details on the remote connectivity configuration.

2.3.2 Device Data

This helps the GE FE manually enter site information (Hospital data). This type of information must be available remotely, especially since the server itself will not be easily physically accessible in most installations. Using information from this tool and GIB Data, Remote Service can login and quickly find product locator information to support system upgrades and tracking activities.

2.3.3 Contact

This is where the FE enters all available site contact information. There are three built-in roles here (**Hospital IT**, **GE Online Center**, and **Hospital Admin**), but additional roles can be added to suit the particular site's contact environment.

2.3.4 ST Language

This sets the Service Tools language for the Customer. English is always displayed for Service user. *Admin*, *Standard*, and *Limited* users will see whatever language is selected here.

2.3.5 Time Settings (NTP)

There are two tabs on this page:

- *Date/Time*: First you shall use this tab to set or check the server's date and time.
- *Time Server*: Then if the site IT has a network time server, use this tab to enter the IP address, hostname or FQDN of the time-server. This allows the AW Server to synchronize its time with the site's network.

NOTICE

An NTP server must be specified in the configuration of servers in a cluster (Scalability enabled). - The same NTP server IP address or hostname has to be set on each node. - The hypervisor shall also use the same NTP Server.

NOTE

On a Virtual Machine, the date and time configured using this Service Tools menu might be overwritten at time of reboot. The reason is that the Virtual Machine is sometimes synchronizing its date and time with the hypervisor. If this issue appears, check the hypervisor settings with the IT admin.

NOTE

GEHC strongly recommends that if enterprise authentication is used, NTP should also be used. **Variable compute loading of the server can cause time drift.** Enterprise authentication relies on time synchronization, and therefore will be problematic if time drift is present. Specifically, if there is more than a 5-minute difference between the Enterprise authentication server and the AW Server, the client will fail login with an error indicating that the server or EA3 is not configured correctly, and the EA3 enterprise test login tool will indicate a "time skew" between the AW Server and the enterprise authentication server.

NOTE

Some NTP servers are available over the Internet and may not be accessible from servers on a hospital network, as a Direct IP address access is needed.

As a reference resource only, for sites that are contemplating using their Windows environment to set up **NTP** - at the time of this writing - Tech Notes on "Windows" time Service Tools can be accessed at <http://technet.microsoft.com/en-us/library/cc773263%28v=ws.10%29.aspx>

The **Check IP** button does a simple ping of the IP address entered. This is a quick and convenient first-level troubleshooting method to see if the entered IP address is reachable on the network

The **Add** button adds the server in the list of NTP servers.

The **Remove** button removes the selected server from the list of NTP servers.

If several servers are listed in this menu, the ntp client of AW Server will try to retrieve the date and time from the first NTP server. If it is not available, the second ntp server will be used and so on until date and time is retrieved.

NOTE

NTP configuration BACKUP/RESTORE is implemented in the default settings. The following settings file is restored unless manually deselected by the user during the restore: /etc/ntp.conf

The status of the NTP Server is also indicated on the HealthPage (in the Software Subsystem section).

To verify the status of the ntp daemon, execute the following command at the Terminal command prompt:

- From AW Server 3.2 Ext. 4.0:

```
systemctl status chronyd <Enter>
```

- For AW Server 3.2 Ext. 3.4 and previous versions:

```
service ntpd status <Enter>
```

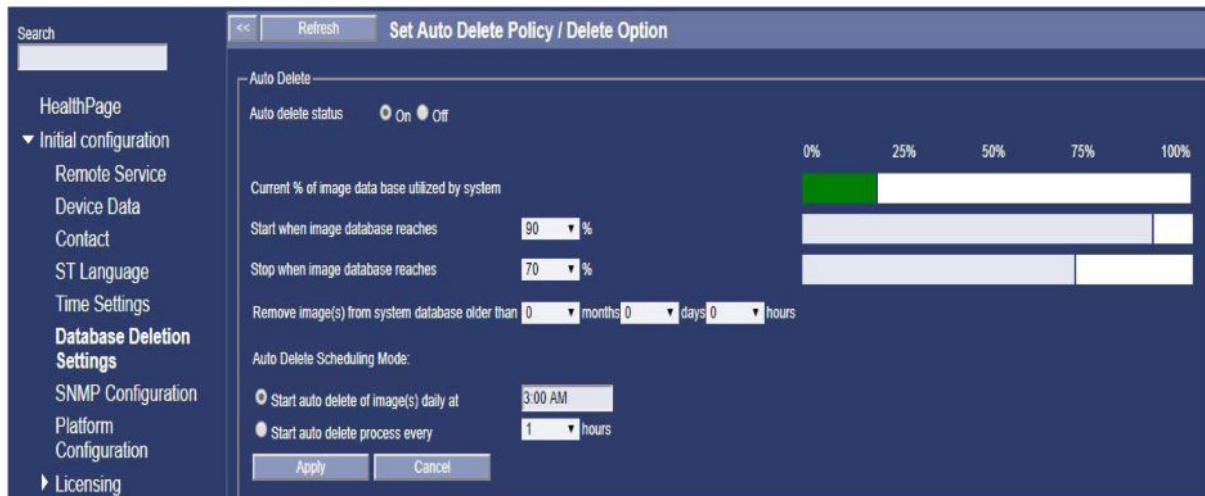
2.3.6 Database Deletion Settings

NOTE

This menu was previously called Auto Delete. It still contains Auto Delete configuration, but it also contains additional parameters for database deletion.

2.3.6.1 Auto Delete Settings

This screen lets you configure how the system automatically deletes older patient image files (This feature can help prevent the image disks from becoming too full). Auto-delete can be configured by the FE at time of installation, subject to approval by the customer or the IT administrator. **This menu is NOT customer configurable.**



A graphical dashboard shows how much image storage is currently used, and if the feature is enabled it shows the storage size limits at which deletion starts and ends.

Auto Delete Rules

When Auto Delete triggers, the following rules are checked in the order listed, to find whether exam is eligible for delete.

- Exam does not have any derived images OR
- Exam has derived images but storage commitment flag has been set OR
- Exam has derived images but are older than the specified age.

Exams that meet above criteria are considered for delete in the decreasing order of their install age (i.e. oldest first).

2.3.6.2 Delete option for worklist browser

When "**Delete option status**" is "**On**", all users except limited users are able to delete exams and series from the AWS client browser. By default this setting is set to "**Off**".



Each exam or serie deletion is logged in a file and is also tracked by audit trail (EAT).

Serie or exam deletion will fail if the exam/serie is:

- currently locked with the "Locked" flag
- currently opened by any user
- currently being transferred (retrieved or pushed)

NOTE

In case of hybrid integration, deleting series or exams on AWS does not delete the exam or series on the PACS system.

NOTE

In case of Full, Seamless or DICOM Direct Connect integration, the "**delete option status**" settings is not available.

For more details on how to delete exams or series from the AWS worklist, please refer to **AW Server 3.2 User Guide** (online help). This document is available in Service Tools in "**Documentation > Documentation**" menu.

2.3.7 Configuring SNMP

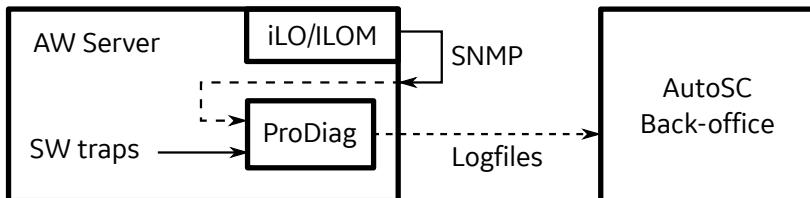
Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment (eg. routers), or computer equipments.

This application works in the background and has neglectable effect on available resources.

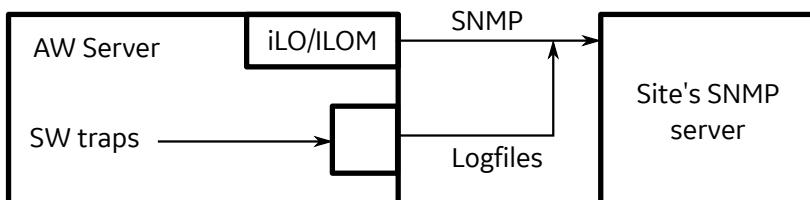
SNMP is used for two different purposes:

- Monitor hardware status by using SNMP capability of the iLO service processor (if applicable). Services are setup to accept traps from the service processor if the SNMP traps is configured in iLO. The IP address of the monitoring server (SNMP server) shall be setup in the iLO configuration page. This is fully described in the AW Server 3.2 Installation and Service Manual, Job Card IST015 - Final Settings.
- Watchdog service is running on AWS, that can also send SNMP traps if it is configured in **Service Tools > Initial configuration > SNMP configuration**. Issues found by the Watchdog are automatically logged. If SNMP trap is configured, it can also send those traps to the monitoring SNMP server. This is fully described in the AW Server 3.2 Installation and Service Manual, Job Card IST008 - Initial Configuration.

SNMP configuration with ProDiag



SNMP configuration with site's SNMP server



NOTE

For EDS, the AW Server is monitored using Centricity OnWatch (refer to the PACS integration documentation).

To configure SNMP:

1. From *Service Tools*, select **Initial configuration > SNMP Configuration**.
2. On the *Simple Network Management Protocol* page, click on the **Enabled** radio button to monitor SNMP traps from the AW Server.

Simple Network Management Protocol

SNMP trap configuration: Enabled Disabled

Monitoring server IP address: awserver

SNMP Community: awserver

Free disk space necessary (%): 25

Buttons: Apply, Cancel

AWS Architecture Diagram:

```

graph TD
    subgraph AWS [AWS]
        AWServer[AW Server]
        ILO[ilo or VM console]
        SM[service management]
        SNMPC[SNMP client]
        APP[applications]
        PL[platform]
        
        AWServer --- ILO
        ILO --- SM
        SM --- SNMPC
        APP --- SM
        PL --- SM
        SNMPC --- NMS["NMS - Monitoring server  
(GE/customer)"]
        
        ILO -. "in case of ILO" .-> NMS
    end
    
```

NOTE

If you chose **Disabled**, skip the next steps and jump to the next section.

3. In **Monitoring server IP address**, enter:
 - the IP address of the site's SNMP server, if there is any.
 - or the AW Server IP address.
4. Click on **Check IP** to verify the TCP/IP connection.
5. Keep **SNMP Community** to awserver to allow the SNMP server to access information on the AW Server.
6. To use the configured SNMP server to monitor the free disk space available, enter the percentage of the required free disk space in the **Free disk space necessary (%)** field. If the free disk space is less than the percentage set, a message is sent to the SNMP server.
7. Click on **Apply** to save the configuration.

NOTE

The service processor must also be configured. See [7.8 HP Escalation and Communication Flow on page 464](#).

NOTE

iLO is not available for virtual AW Servers.

2.3.8 Platform Configuration

The Platform Configuration menu is used to configure the following:

- Platform License can be configured in the Platform Configuration tab.
- Scalability mode can be configured in the Scalability tab.
- Integration mode can be configured in the Integration tab.

The three tabs have to be configured consecutively. After entering the correct settings in each tab, navigate to the last tab “Integration” and hit the **Apply** button to save all changes.

NOTICE

If you modify some settings without clicking the Apply button in the last tab, your modifications will be lost.

NOTICE

Maintenance Mode is needed to make any change to the Platform Configuration. Before entering a platform license or configuring integration, ensure that the AW Server is in Maintenance Mode. Refer to [4.2.2 Start Maintenance Mode on page 389](#) for more details on Maintenance Mode.

The below table displays all the available configurations for the physical and virtual AW Server:

Hardware				Users, Licenses, Integration Modes							
Tier	HW platform	Core s	RAM	Users	Slice Count licenses	Apps 2 cores/App	No Integ	Hybrid	Seamless (UV)	Dicom Direct Connect	
Physical LT	HP ML 350 - G6 NOTE Not supported from AWS3.2 Ext. 4.0.	12	24 GB	10	8k - SdC_Server_Two_Seats	~6	OK	OK	---	---	
			64 GB		40k - SdC_Low_Tier_Premium		OK	OK			
	HP ML 350p - G8	12	24 GB		8k - SdC_Server_Two_Seats	~6	OK	OK			

Hardware				Users, Licenses, Integration Modes							
Tier	HW platform	Cores	RAM	Users	Slice Count licenses	Apps 2 cores/App	No Integ	Hybrid	Seamless (UV)	Dicom Direct Connect	
	NOTE Not supported from AWS3.2 Ext. 4.8.		64 GB		40k - SdC_Low_Tier_Premium		OK	OK			
	HP DL360 - G9	20	64 GB		40k - SdC_Low_Tier_Premium	~10	OK	OK			
	HP DL360 - G10	20	96 GB		40k - SdC_Low_Tier_Premium	~10	OK EC supported	OK EC supported			
Physical HT	HP DL 580 - G7	24	64 GB	50	16k - SdC_Server_Four_Seats	~12	OK	OK	---	---	
	NOTE Not supported from AWS3.2 Ext. 4.2				40k - SdC_Server_Eight_Seats		OK	OK			
	HP DL 560 - G8	32	64 GB		16k - SdC_Server_Four_Seats	~16	OK	OK			
	NOTE Only configuration with min 300 GB disk size is supported from AWS3.2 Ext. 4.2				40k - SdC_Server_Eight_Seats		OK	OK			
	NOTE Not supported from AWS3.2 Ext. 4.8.			256 GB	80k - SdC_High_Tier_Standard	~16	OK	OK	---	---	
	HP DL360 - G9	32	256 GB		160k - SdC_High_Tier_Premium		OK	OK			
					80k - SdC_High_Tier_Standard	~16	OK From AWS 3.2 Ext. 4.8 EC supported	OK			

Hardware				Users, Licenses, Integration Modes							
Tier	HW platform	Cores	RAM	Users	Slice Count licenses	Apps 2 cores/App	No Integ	Hybrid	Seamless (UV)	Dicom Direct Connect	
	HP DL360 - G10	36	384 GB		160k - SdC_High_Tier_Premium		OK From AWS 3.2 Ext. 4.8 EC supported	OK			
					80k - SdC_High_Tier_Standard	~16	OK EC supported	OK EC supported		OK From AWS 3.2 Ext. 4.9 EC supported	
					160k - SdC_High_Tier_Premium		OK EC supported	OK EC supported		OK From AWS 3.2 Ext. 4.9 EC supported	
VM-LT	Any	8	24 GB	10	8k - SdC_Server_Two_Seats	~4	OK	OK	---	---	
				25	16k - SdC_Server_Four_Seats	~4	---	---	OK clustering supported	---	
				25	40k - SdC_Low_Tier_Premium	~4	---	---	OK clustering supported From AWS 3.2 Ext. 4.4	---	
				10	40k - SdC_Low_Tier_Premium	~4	OK From AWS 3.2 Ext. 4.2	OK From AWS 3.2 Ext. 4.2	---	OK clustering supported	
				10	40k - SdC_Low_Tier_Premium	~4	OK From AWS 3.2 Ext. 4.2 EC supported	OK From AWS 3.2 Ext. 4.2 EC supported	---	OK From AWS 3.2 Ext. 4.2 EC supported without clustering	

Hardware				Users, Licenses, Integration Modes							
Tier	HW platform	Cores	RAM	Users	Slice Count licenses	Apps 2 cores/App	No Integ	Hybrid	Seamless (UV)	Dicom Direct Connect	
			12 GB	1	4k - SdC_Nano_4k	~4	---	---	---	OK without clustering	
			26 GB	1	12k - SdC_Nano_12k	~4	---	---	---	OK without clustering	
			32 GB	1	16k - SdC_Nano_16k	~4	---	---	---	OK without clustering	
			32 GB	N/A	16k - SdC_Server_Four_Seats (for web access)	N/A	OK Only AWS 3.2 Ext. 3.6	---	---	---	
VM-HT	Any	24	64 GB/ 72 GB**	30/50 **	40k - SdC_Server_Eight_Seats	~12	OK	OK	---	---	
			104 GB	50	40k - SdC_Server_Eight_Seats	~12	OK From AWS 3.2 Ext. 4.2 EC supported	OK From AWS 3.2 Ext. 4.2 EC supported	---	OK From AWS 3.2 Ext. 4.9 EC supported	
			64 GB	50	40k - SdC_Server_Eight_Seats	~12	---	---	OK	---	
Supported on all configurations				160k - SdC_Server_Eight_Seat_DEMO							

*For Seamless 24 GB minimum, 32 GB recommended

**Up to AW Server 3.2 Ext. 3.4: 64 GB RAM and 50 concurrent logins.

From AW Server 3.2 Ext. 4.0:

- VM-HT with 64 GB RAM supports 30 concurrent logins,
- VM-HT with 72 GB RAM supports 50 concurrent logins.

The Platform Configuration is fully described in the AW Server 3.2 Installation Manual (or Installation and Service Manual), Job Card IST008, Platform Configuration.

2.3.9 Licensing

NOTE

Note that the licenses configured hereafter with the **Licensing tool are all “Node locked” licenses**. Floating licenses for the Applications will be setup by the Administrative/Configuration tool.

NOTICE

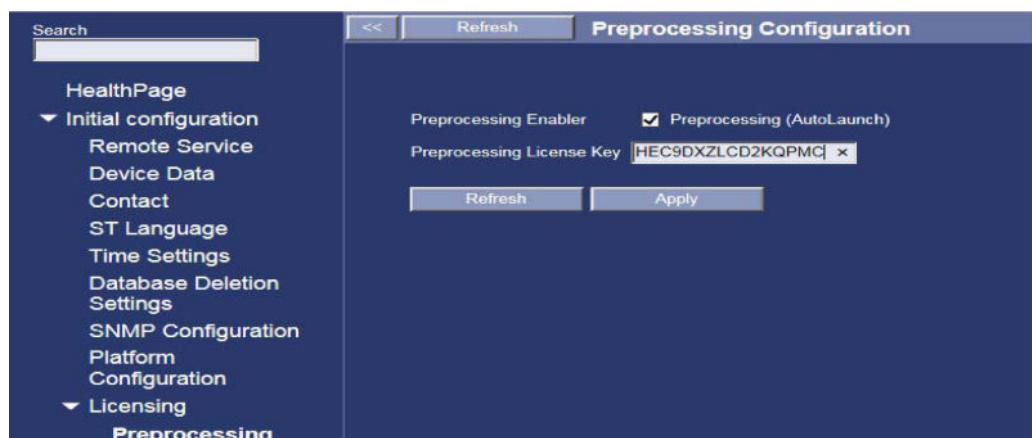
Ensure that licenses are generated using the correct Model Type for the server (AWS_Primary or AWS_Node).

2.3.9.1 Activating the preprocessing application (AutoLaunch)

If the site has purchased the Preprocessing application (also called AutoLaunch), a one node-locked Preprocessing license key is received.

1. In Service Tools, select **Initial Configuration > Licensing > Preprocessing**.

The *Preprocessing Configuration* panel appears.



2. Click on the **Preprocessing Enabler** check-box to enable the application.
3. Enter the license key in the **Preprocessing License Key** field.
4. Click on the **Apply** button to save.

NOTE

Preprocessing must also be configured in the **Administrative > Configuration > Preprocessing** screen (which is not available until the details above are entered).

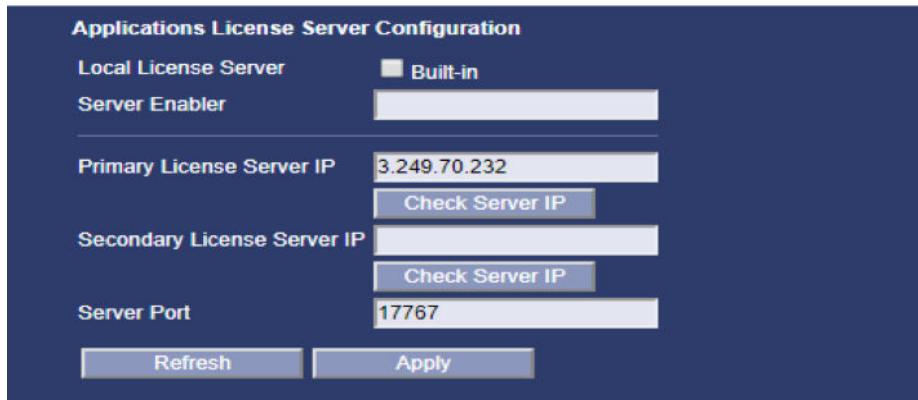
For an explanation of this feature, see the AW Server 3.2 Installation and Service Manual, Preprocessing Configuration.

2.3.9.2 MailSender

The MailSender allows applications which use email service to send email reports to predefined contacts/recipients.

For more details, refer to the AW Server 3.2 Installation and Service Manual, MailSender.

2.3.9.3 CoLA Server Configuration



The AW Server is setup to use only Floating Licenses for its advanced applications. It can be configured to use licenses from one of two sources, a built-in license server, or external license server(s):

1. Server Configuration – Built-in

The server can act as a Floating License CoLA server for its own internal advanced applications, and for external AW resident advanced applications.

- To configure the built-in server, click the **Built-in** button, acquire the **Server Enabler license** from eLicense (CoLA_License_Server), and enter the license in the **Server Enabler** field.
- Then click **Apply**.

A pop-up box will appear indicating a successful/valid license, or a failure on an invalid license.

- A **GREEN** indication appears next to the license field if the license is valid and the server is OK.

The status of the built-in FL server is also indicated on the **HealthPage** of the Service Tools. In the Software Subsystem section, the **Built-in License Server (cola)** refers to the built-in FL server.

OK means it is configured with a valid server enabler and is running.

- A **RED** indication means the software service is failing **or is not running**.
- A **GRAY** “not in use” indication means it is not selected, and not being used.

NOTE

When checking the "Built-in" button, the "Primary License Service IP" is changed to 127.0.0.1 by default. This is the local IP address of the AW Server. It is possible to change this value to use an external license server as primary license server.

2. Server Configuration – External

The server can also be configured to use an existing **external Floating License Server** already in use on the network.

- Select “External” and enter the **IP address** of the Primary and Secondary external FL servers to be used (Secondary server is optional).

The port used by external server communication has a default value = **17767** (This may be reconfigured).

- Click on **Check IP** to make sure the server is connected and/or reachable. No need for the Server Enabler license.

If the **Check Server IP** is successful, this means that the IP address entered is valid and reachable. **It does not mean that the IP address is a functioning Floating License server.**

NOTE

The recommended configuration is to use the internal Floating License Server. Alternatively, an external Floating License Server can be used, especially if there are multiple AW Server and AW Workstations at the same site.

NOTE

It is possible to configure a built-in Primary license server, and an external Secondary external license server.

NOTE

A secondary License server acts as a back-up server to be used when the primary server is down, to the extent that license keys for the same applications are installed on both. Customer needs to purchase a specific CAT Number in order to get licenses for the Secondary License Server. In this case the primary and secondary license servers will have exactly the same list of licenses. Details on generating the licenses for the secondary license server are available in eLicense User Guide.

NOTE

For clustered servers (configured in Scalability) it is recommended to install two external license servers on PCs. Failing this, it is possible to install two of the cluster nodes as license servers.

2.3.9.4 Floating License Configuration

To manage Application Licenses installed on the selected Application License Server(s), use the Floating License Manager tool (**Initial Configuration** > **Licensing** > **Floating License** menu in Service Tools). This tool is fully described in the AW Server 3.2 Installation and Service Manual, Job Card IST008.

2.3.10 Scalability

Select the **Scalability** option from the **Initial Configuration** menu of the Service Tools to display the screen. Use it to manage aspects of server scalability:

- to review a dashboard of servers potentially forming part of the cluster and their current states.
- to define the "Golden Set" which is used as a reference configuration by servers in the cluster.
- to remove an inactive node from the cluster.

NOTE

This is not available for physical AW Servers. If you access this option on a physical server, the following message will display: **Cluster mode is available only for virtual machines**

A cluster can be composed of a maximum number of AW Server nodes (the maximum number of nodes is defined in the AW Server 3.2 Pre-Installation Manual and the AW Server 3.2 Installation and Service Manual). The requirements are the following:

- each AW Server node should have the same configuration as the golden set (list of applications, platform version, ...)
- each AW Server node should have a second network card connected to the private cluster network.

2.3.10.1 Cluster dashboard

An example screen for a simple cluster configuration is shown below:

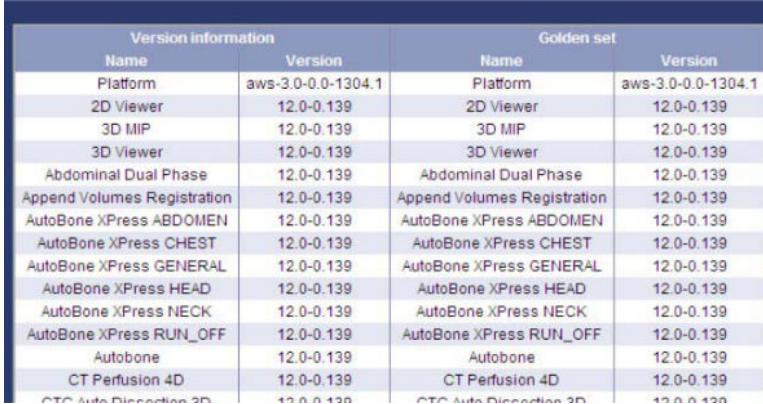
The screenshot shows a cluster configuration interface. At the top, it displays the host name as 'virt244' and cluster settings as 'Single Mode'. Below this is a table of known nodes:

NODE [IP ADDRESS]	CLIENTS	APPLICATIONS	SLICES	CPU	MEMORY	DISK	VERSION	LICENSE SERVER
virt243 [3.213.154.243] [10.0.248.243]	0	0	0	9%	787MB / 3829MB (21%)	/dev/sda2 13GB / 57GB (23%) /dev/sda3 0GB / 9GB (0%)	OK	P: 127.0.0.1 S: 3.213.154.244
virt244 [3.213.154.244] [10.0.248.244]	0	0	0	4%	770MB / 3829MB (21%)	/dev/sda2 13GB / 57GB (23%) /dev/sda3 0GB / 9GB (0%)	OK	P: 3.213.154.243 S: 3.213.154.244

In the lower part of the screen you will see a dashboard of server details for the server and any others which actually or potentially form part of a cluster (known nodes).

The columns in this table provide the following information and functionality:

Column name	Purpose
Node IP Address	<p>This column indicates the known server nodes' IP addresses, hostnames and their statuses (whether a node is active, in maintenance mode, if it is the preference server, or if it has a problem affecting its participation in the cluster):</p> <p>Indicates the list of known nodes in the cluster, displaying the host name and the IP addresses of each node. The status of the node is indicated with icons:</p> <ul style="list-style-type: none"> ✓ node is active (broadcast information received) ⚠ there is a problem with the preference servers ✗ node is in Maintenance Mode ⚠ node has some problem ✗ node is inactive (no broadcast information received) <p>Note: The host name is a link also to the Service Tools page of the node.</p> <p>If the server node is inactive (red X icon), no information will be displayed in the other columns for that server.</p> <p>NOTE</p> <p>Active nodes communicate within the cluster via broadcast messages.</p> <p>To access the Service Tools of another node in the cluster, click its host-name hyperlink in this field. The corresponding Service Tools page will then open a new browser window. (Note that it may be necessary to relog on the server when using remote Service Tools like Insite/RSVP with FFA.)</p>
Clients	The total number of clients currently logged onto the server. (Scalability is achieved by assigning users at login time so that they are evenly assigned across nodes on the cluster.)
Applications	The total number of current application sessions running on the server
Slices	The total number of exam slices currently utilized on the server
CPU	The current percentage CPU load on the server (this may exceed 100%). A system has multiple CPU cores (At least 8 vCPUs). A load of 100% means that one CPU core is fully loaded.
Memory	The current RAM memory usage on the server (actual, total, and percentage)
Disk	The server's disk partitions with their current usage (actual, total, and percentage)

Column name	Purpose																																																																				
Version	<p>Shows whether the set of Advanced Applications and their installed versions on the server are compatible with the defined "Golden Set" (target or reference list of apps and versions). Ideally all server nodes in the list will indicate "OK". If the apps installed on a server do not conform with the Golden Set this field will display in red.</p> <p>Click the field to display the detailed list of apps and versions on the server, compared to the current Golden Set (on the right of the list). An example is shown below: Only applications with activated licenses are listed.</p>  <table border="1"> <thead> <tr> <th colspan="2">Version information</th> <th colspan="2">Golden set</th> </tr> <tr> <th>Name</th> <th>Version</th> <th>Name</th> <th>Version</th> </tr> </thead> <tbody> <tr><td>Platform</td><td>aws-3.0.0-0-1304.1</td><td>Platform</td><td>aws-3.0.0-0-1304.1</td></tr> <tr><td>2D Viewer</td><td>12.0-0.139</td><td>2D Viewer</td><td>12.0-0.139</td></tr> <tr><td>3D MIP</td><td>12.0-0.139</td><td>3D MIP</td><td>12.0-0.139</td></tr> <tr><td>3D Viewer</td><td>12.0-0.139</td><td>3D Viewer</td><td>12.0-0.139</td></tr> <tr><td>Abdominal Dual Phase</td><td>12.0-0.139</td><td>Abdominal Dual Phase</td><td>12.0-0.139</td></tr> <tr><td>Append Volumes Registration</td><td>12.0-0.139</td><td>Append Volumes Registration</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress ABDOMEN</td><td>12.0-0.139</td><td>AutoBone XPress ABDOMEN</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress CHEST</td><td>12.0-0.139</td><td>AutoBone XPress CHEST</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress GENERAL</td><td>12.0-0.139</td><td>AutoBone XPress GENERAL</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress HEAD</td><td>12.0-0.139</td><td>AutoBone XPress HEAD</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress NECK</td><td>12.0-0.139</td><td>AutoBone XPress NECK</td><td>12.0-0.139</td></tr> <tr><td>AutoBone XPress RUN_OFF</td><td>12.0-0.139</td><td>AutoBone XPress RUN_OFF</td><td>12.0-0.139</td></tr> <tr><td>Autobone</td><td>12.0-0.139</td><td>Autobone</td><td>12.0-0.139</td></tr> <tr><td>CT Perfusion 4D</td><td>12.0-0.139</td><td>CT Perfusion 4D</td><td>12.0-0.139</td></tr> <tr><td>CTC Auto Dissection 3D</td><td>12.0-0.139</td><td>CTC Auto Dissection 3D</td><td>12.0-0.139</td></tr> </tbody> </table> <p>If versions differ between nodes, identify the node that provides the appropriate version and set it as the Golden Set.</p> <p>To set the server's app list as the new Golden Set for the cluster (if different from the current one), click the corresponding button at the bottom of the list.</p> <p>Click the Hide button to return to the main screen.</p>	Version information		Golden set		Name	Version	Name	Version	Platform	aws-3.0.0-0-1304.1	Platform	aws-3.0.0-0-1304.1	2D Viewer	12.0-0.139	2D Viewer	12.0-0.139	3D MIP	12.0-0.139	3D MIP	12.0-0.139	3D Viewer	12.0-0.139	3D Viewer	12.0-0.139	Abdominal Dual Phase	12.0-0.139	Abdominal Dual Phase	12.0-0.139	Append Volumes Registration	12.0-0.139	Append Volumes Registration	12.0-0.139	AutoBone XPress ABDOMEN	12.0-0.139	AutoBone XPress ABDOMEN	12.0-0.139	AutoBone XPress CHEST	12.0-0.139	AutoBone XPress CHEST	12.0-0.139	AutoBone XPress GENERAL	12.0-0.139	AutoBone XPress GENERAL	12.0-0.139	AutoBone XPress HEAD	12.0-0.139	AutoBone XPress HEAD	12.0-0.139	AutoBone XPress NECK	12.0-0.139	AutoBone XPress NECK	12.0-0.139	AutoBone XPress RUN_OFF	12.0-0.139	AutoBone XPress RUN_OFF	12.0-0.139	Autobone	12.0-0.139	Autobone	12.0-0.139	CT Perfusion 4D	12.0-0.139	CT Perfusion 4D	12.0-0.139	CTC Auto Dissection 3D	12.0-0.139	CTC Auto Dissection 3D	12.0-0.139
Version information		Golden set																																																																			
Name	Version	Name	Version																																																																		
Platform	aws-3.0.0-0-1304.1	Platform	aws-3.0.0-0-1304.1																																																																		
2D Viewer	12.0-0.139	2D Viewer	12.0-0.139																																																																		
3D MIP	12.0-0.139	3D MIP	12.0-0.139																																																																		
3D Viewer	12.0-0.139	3D Viewer	12.0-0.139																																																																		
Abdominal Dual Phase	12.0-0.139	Abdominal Dual Phase	12.0-0.139																																																																		
Append Volumes Registration	12.0-0.139	Append Volumes Registration	12.0-0.139																																																																		
AutoBone XPress ABDOMEN	12.0-0.139	AutoBone XPress ABDOMEN	12.0-0.139																																																																		
AutoBone XPress CHEST	12.0-0.139	AutoBone XPress CHEST	12.0-0.139																																																																		
AutoBone XPress GENERAL	12.0-0.139	AutoBone XPress GENERAL	12.0-0.139																																																																		
AutoBone XPress HEAD	12.0-0.139	AutoBone XPress HEAD	12.0-0.139																																																																		
AutoBone XPress NECK	12.0-0.139	AutoBone XPress NECK	12.0-0.139																																																																		
AutoBone XPress RUN_OFF	12.0-0.139	AutoBone XPress RUN_OFF	12.0-0.139																																																																		
Autobone	12.0-0.139	Autobone	12.0-0.139																																																																		
CT Perfusion 4D	12.0-0.139	CT Perfusion 4D	12.0-0.139																																																																		
CTC Auto Dissection 3D	12.0-0.139	CTC Auto Dissection 3D	12.0-0.139																																																																		
License Server	<p>Lists the Primary (P) and any Secondary (S) license servers defined. Note that a secondary server is compulsory for nodes in Cluster mode, and if none is defined, a red X is displayed in the field.</p>																																																																				

The status of the 2 HAPS nodes is also displayed as follows:

- IP address: private network IP address used to communicate between HAPS nodes and AW Server nodes
- Free disk space
- Total disk space
- Preference directory
- Available: if the HAPS node is up and running, "Y" is displayed. If the HAPS node is not reachable (network issue, HAPS node down...) "N" is displayed.

Highly Available Preference Storage (HAPS)				
IP address	Free disk space	Total disk space	Preference directory	Available
192.168.1.223	28.3GB	31.4GB	/var/awsprefs	Y
192.168.1.222	28.3GB	31.4GB	/var/awsprefs	Y

2.3.10.2 Node removal

When troubleshooting a cluster, it is possible to remove one node from the cluster:

- Tick the checkbox for the node you want to remove. This is only possible if the node is inactive.
- Select "Delete selected nodes".

This feature is used to "clean" the list of nodes in the cluster. For example when one node changes its IP address, two lines are indicated in the dashboard: one for the old IP address, and another for the new. The node removal feature enables to clean the unused IP address.

2.3.11 Audit Trail (EAT)

This tool is used to manage and keep track of authentication log histories, and trails – EAT – **Enterprise Authentication Trail**. The interface has 3 tabs – **Local**, **Repository**, and **Viewer**. Use the **Viewer** tab to view login authentication history. **EAT is enabled by default.**

The **Local** and **Repository** tabs are available for site IT purposes if required.

In the viewer, clicking on a line will pop-up the raw data associated with the log entry; clicking outside the box will close the data pop-up.

Figure 2-1 AUDIT TRAIL (EAT) TOOL LOCAL

The screenshot shows the Audit Trail (EAT) tool interface. On the left, there is a navigation tree with the following structure:

- HealthPage
- Initial configuration
 - Remote Service
 - Device Data
 - Contact
 - ST Language
 - Time Settings
 - Database Deletion Settings
 - SNMP Configuration
 - Platform Configuration
- Licensing
- Scalability
- Audit Trail (EAT)

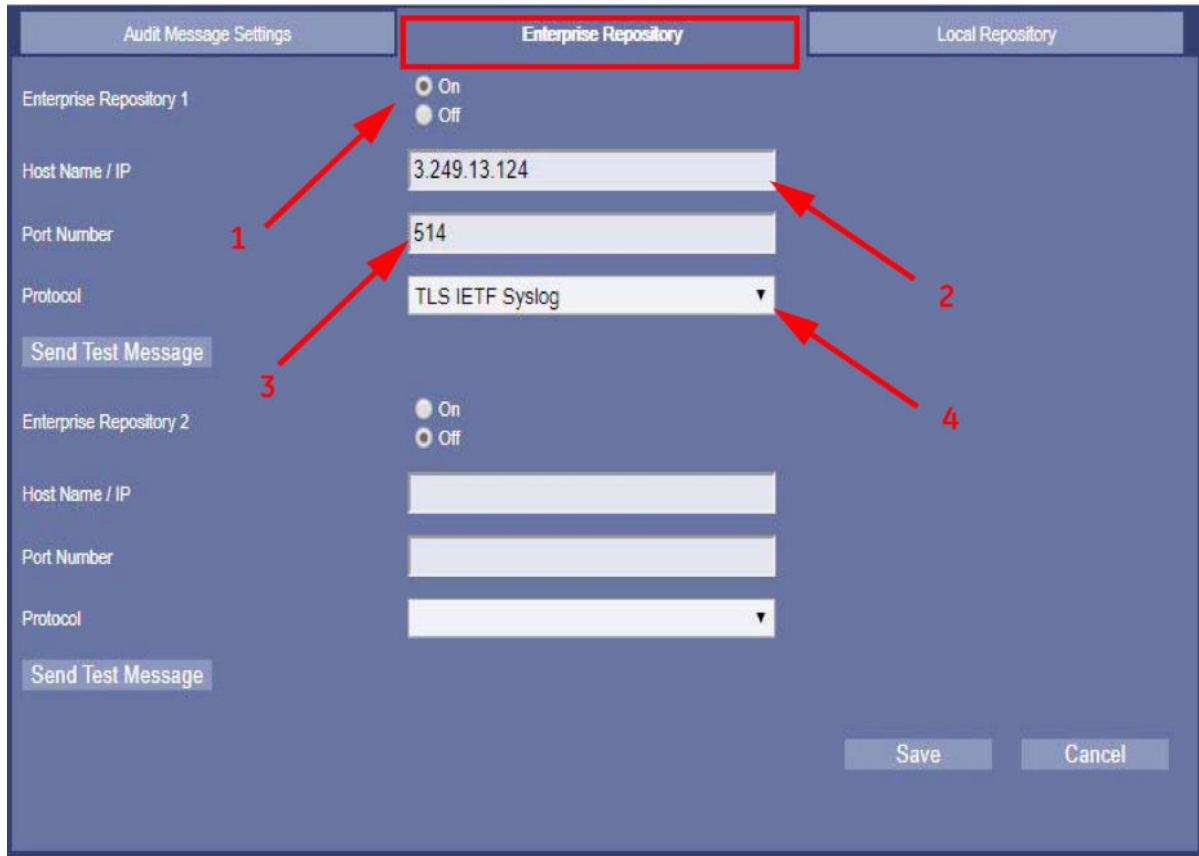
The main area has three tabs at the top: **Audit Message Settings** (highlighted with a red box), **Enterprise Repository**, and **Local Repository** (also highlighted with a red box). The **Audit Message Settings** tab contains fields for **Audit Source ID** (a dropdown menu), **Patient Name Anonymized** (with radio buttons for **On** and **Off**), and buttons for **Save** and **Cancel**.

The **Local Repository** tab is currently active. It shows a list of events under the heading **Event ID / Time / Event Outcome**. The first event listed is:

```
110114 [2019-02-22T10:22:21] Success
```

Below the list are buttons for navigating through the pages (Page 1 / 2) and a link to **Display Raw XML**.

To the right of the event list, there is a detailed view of the selected event (Event ID 110114). It includes sections for **Event** (Event Date/Time, Event ID, Event Action Code, Event Outcome Indicator, Event Type Code, Event Original Text) and **Active Participant** (User ID, User Name, User Is Requestor).

Figure 2-2 AUDIT TRAIL (EAT) TOOL ENTERPRISE

If the site wants to use its Enterprise Repository for Audit trails, proceed with the following:

1. Enable the Enterprise repository
2. Enter the Enterprise repository Hostname or IP address
3. Enter the Enterprise repository Port number
4. Select the Enterprise repository Protocol

Request this information from the IT administrator of the site.

2.3.12 Prodiag

The Prodiag (Proactive Diagnostics) feature manages logfiles and scheduled diagnostic tasks. It is **pre-configured** to be used with AW Server. **It does not require additional configuration.** However it is only useful to export data when remote connectivity (InSite/RSvP) is available on the server (GEHC Service only).

NOTE

Prodiag connectivity relies on InSite/RSvP connectivity. InSite/RSvP is not used by EDS, therefore for AW Server configurations such as Seamless Integration with Universal Viewer, Prodiag will not be available remotely.

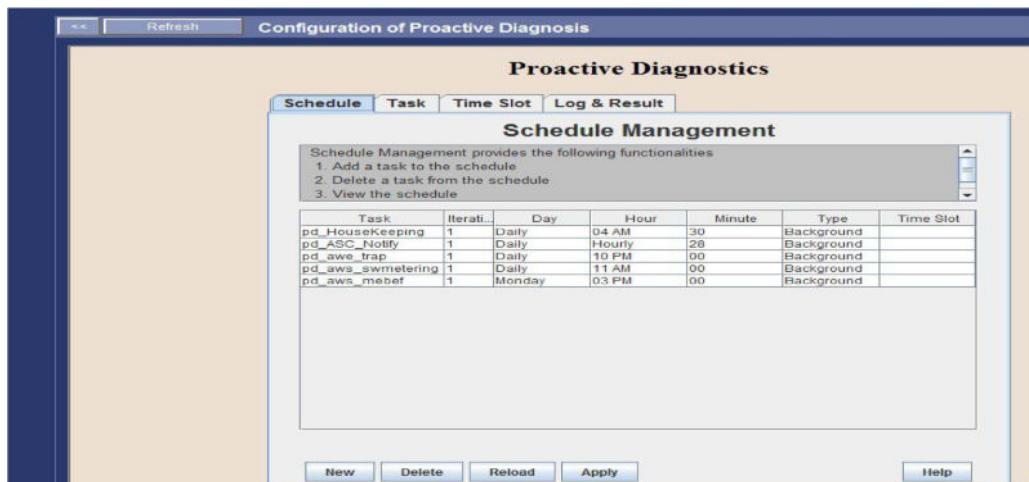
NOTE

However, Prodiag will be active even if AW Server is in PACS Backend configuration mode. It will still run in the background, but if not connected to the “backoffice” via InSite/RSvP, the logfiles will simply not be sent.

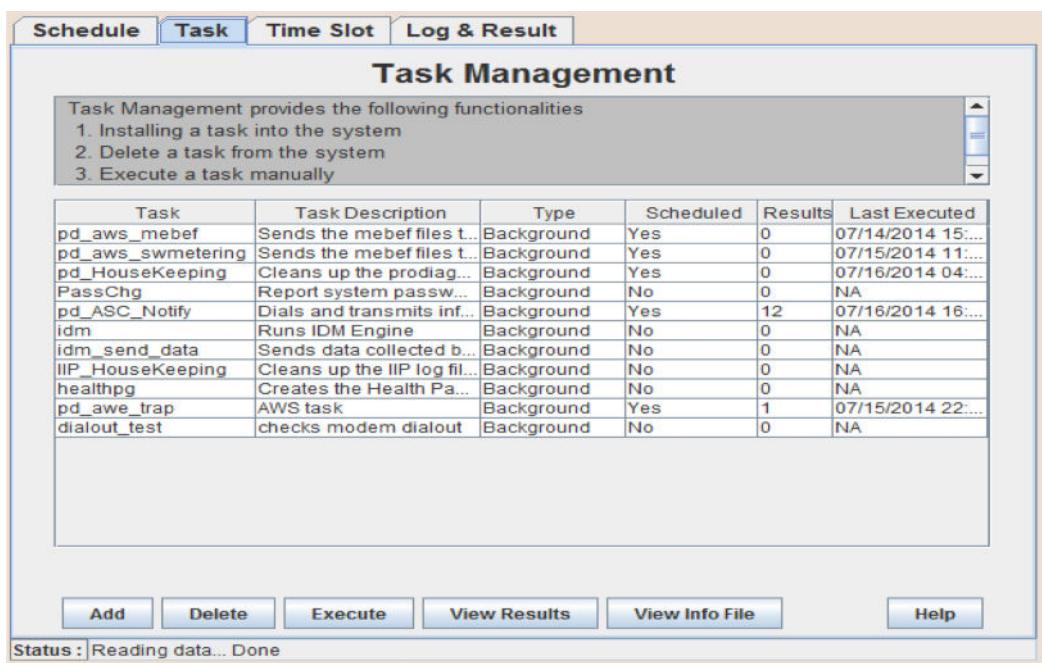
2.3.12.1 Prodiag management with InSite

For AW Server versions prior to AW Server 3.2 Ext. 4.2, Prodiag is managed using the Proactive Diagnostics tool:

1. To open the menu, click on **Prodiag**. A Java™ pop-up may be displayed, in which case, select OK. The **Proactive Diagnostics** tool should display as shown in the following illustration.



A number of tasks are available from the **Task** tab.



2. To execute a task manually, click the **Execute** button. Otherwise, tasks can be scheduled for regular execution on the **Schedule** tab.
3. To **add** a new task to the system, click Add and specify the path to the task file.
4. Make any modifications that would be needed (i.e: change time for an event, or add new events) then click **Apply** to save and exit.

2.3.12.2 Prodiag Management with RSvP

For AW Server versions from AW Server 3.2 Ext. 4.2, Prodiag is managed through command lines.

NOTE

The Prodiag feature is enabled by default. If it is not the case, enable it from the Service Tools as described in the Installation Manual *Job Card IST008 – Remote Service*.

1. Open the AW Server Console/terminal, login as **root**.

2. To display the Prodiag tasks that are available on the AW Server, type the command:

```
ProdiagScheduler.py results <Enter>
```

An XML output displays with the Prodiag tasks data (in the example below there are two Prodiag tasks):

```
[root@bucaw70-243 ~]# ProdiagScheduler.py results
<?xml version="1.0" ?>
<Scheduler>
  <IntrusiveCheckScript/>
  <JobList NextAvailableID="2">
    <Job id="0">
      <ScriptSetName>pd_awe_trap</ScriptSetName>
      <Cron>0 22 * * * </Cron>
      <FirstRunDatetime>2021-01-14T22:00:00</FirstRunDatetime>
      <LastRunDatetime>2021-01-26T22:00:01</LastRunDatetime>
      <LastRunResult>0</LastRunResult>
      <NextRunDatetime>2021-01-27T22:00:00</NextRunDatetime>
    </Job>
    <Job id="1">
      <ScriptSetName>pd_aws_mebef</ScriptSetName>
      <Cron>0 15 * * 1 * </Cron>
      <FirstRunDatetime>2021-01-18T15:00:00</FirstRunDatetime>
      <LastRunDatetime>2021-01-25T15:00:01</LastRunDatetime>
      <LastRunResult>0</LastRunResult>
      <NextRunDatetime>2021-02-01T15:00:00</NextRunDatetime>
    </Job>
  </JobList>
  <ScriptSetList>
    <ScriptSet name="pd_awe_trap">
      <MainScript>pd_awe_trap</MainScript>
      <ScriptSetJobList>
        <Job id="0"/>
      </ScriptSetJobList>
      <Background>Yes</Background>
      <Timeout>3000</Timeout>
    </ScriptSet>
    <ScriptSet name="pd_aws_mebef">
      <MainScript>pd_aws_mebef</MainScript>
      <ScriptSetJobList>
        <Job id="1"/>
      </ScriptSetJobList>
      <Background>Yes</Background>
      <Timeout>1000</Timeout>
    </ScriptSet>
  </ScriptSetList>
</Scheduler>
```

- This command displays the schedule of the Prodiag tasks.

In the example above, the schedule of the “pd_awe_trap” task is circled in red.

- This command displays the results of the Prodiag Scheduler run

In the example above, the results and the running date of the “pd_aws_mebef” run is circled in green.

- This command displays the tasks description.

In the example above, the description of the “pd_awe_trap” task is circled in blue.

3. To add a schedule for a Prodiag task in the scheduler, type the command:

```
ProdiagScheduler.py addtask -scriptname <ScriptName> -scheduletime
<Schedule> <Enter>
```

E.g: Adding a schedule for “pd_awe_trap” task:

```
ProdiagScheduler.py addtask -scriptname "pd_awe_trap" -scheduletime "M
12:00AM" <Enter>
```

The second schedule of the “pd_awe_trap” task displays when typing the command to display the Prodiag tasks in [Step 2](#).

```
<Job id="2">
  <ScriptSetName>pd_awe_trap</ScriptSetName>
  <Cron>00 * * 1 *</Cron>
  <FirstRunDatetime>2021-02-01T00:00:00</FirstRunDatetime>
</Job>
```

4. To modify a schedule for a Prodiag task in the scheduler, type the command:

```
ProdiagScheduler.py modifytask -jobid <jobid> -scriptname <ScriptName>
-scheduletime <Schedule> <Enter>
```

E.g: Modifying the schedule, previously created for “pd_awe_trap” task:

```
ProdiagScheduler.py modifytask -jobid 2 -scriptname "pd_awe_trap"
-scheduletime "M 03:00AM" <Enter>
```

The second schedule of the “pd_awe_trap” task has changed when typing the command to display the Prodiag tasks in [Step 2](#).

5. To remove a schedule for a Prodiag task in the scheduler, type the command:

```
ProdiagScheduler.py rmtask -jobid <jobid> <Enter>
```

E.g: Removing the schedule, previously created for “pd_awe_trap” task:

```
ProdiagScheduler.py rmtask -jobid 2 <Enter>
```

The second schedule of the “pd_awe_trap” task has been removed when typing the command to display the Prodiag tasks in [Step 2](#).

6. To re-register the default schedules for the Prodiag tasks (if they were removed from Prodiag Scheduler), execute the following scripts:

```
/export/home/sdc/scripts/pd_awe_trap_schedule <Enter>
```

```
/export/home/sdc/scripts/pd_awe_mebef_schedule <Enter>
```

2.3.13 GIB Data

- Use the GIB Data Tab to enter registration information from each product locator card. **Ensure that you complete all data fields.** This information is saved on the system and may be viewed at any time.
- Send the GIB data to GEHC online by clicking on the **Send via PC** button. This will ensure proper traceability and service. **As long as GIB data is not sent, a message will be displayed at the top of Service Tools screen.** Alternatively, the **Send via email** option composes an email. If the PC is not connected to GE mail, the email can be sent later.

This must be done each time the configuration on the server is modified (for example packages added, removed or updated...). Refer to Chapter 5, [5.3.8 Registration on page 429](#).

2.3.14 AUM Configuration

Refer to [2.4.2.4 Application Usage Data on page 84](#).

2.4 Administrative Options menu

The options on the Administrative menu in the Service Tools are described below.

2.4.1 Configuration

The following **Administrative > Configuration** options are fully described in the AW Server 3.2 Installation and Service Manual, Job Card IST010 - Administrative Configuration:

- DICOM Hosts
- DICOM Printers
- PostScript printers
- Users (EA3)
- Smart Card Configuration
- Client Timeout
- Preprocessing
- MailSender
- End Of Review

NOTE

Starting from AW Server 3.1, the **Floating License** menu is now in **Initial Configuration > Licensing**.

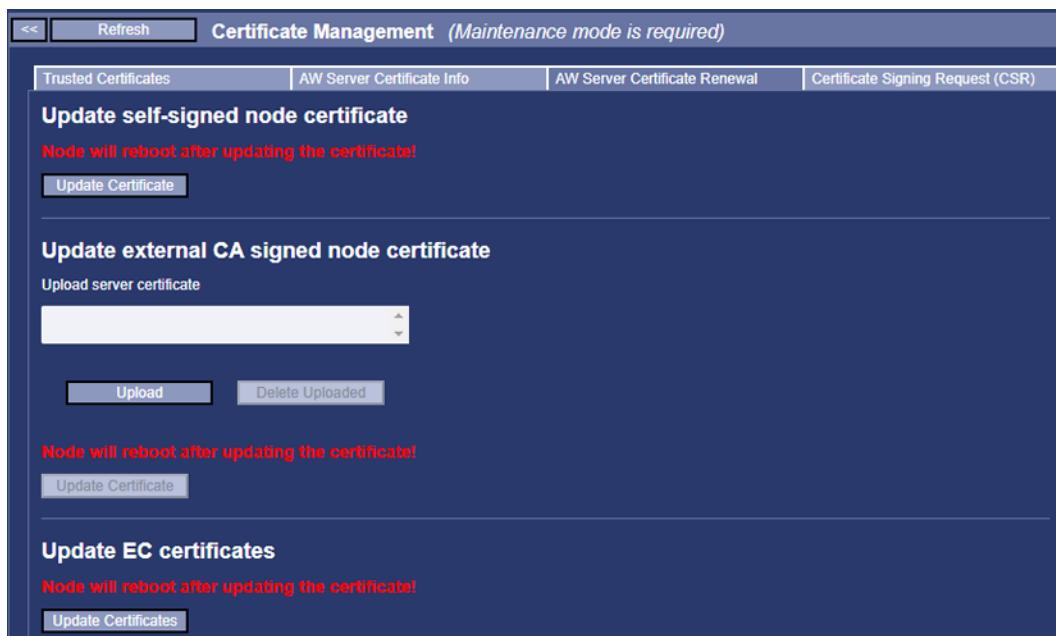
2.4.1.1 Certificate Management

This section is related to the management of the certificates files, from AW Server 3.2 Ext. 4.2, using the Service Tools Certificate Management page.

This section describes the renewal of the AW Server self-signed certificate and Web Client certificate (for AW Server 3.2 Ext. 4.2, Ext. 4.4 and Ext. 4.6).

The other certificate management features are fully described in the *AW Server 3.2 Installation Manual, Job Card IST010 - Administrative Configuration* and the section [A.21 Installing/renewing an AW Server external CA signed certificate on page 514](#).

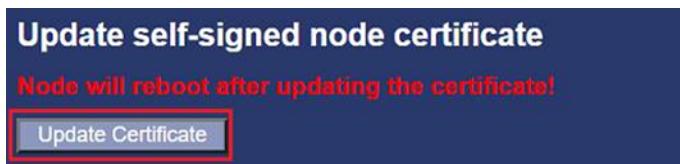
From the Service Tools, select **Administrative > Configuration > Certificate Management**, and select the **AW Server Certificate Renewal** tab.

**NOTE**

In the below procedure you will be asked to reboot the AW Server for each certificate update.

2.4.1.1.1 Renewing AW Server self-signed certificate

- In the *Update self-signed node certificate* part of the page, click on **Update Certificate**.



- In the warning message that displays, confirm the removal of the previous certificate and the installation of the new certificate.



- In the warning message that displays, confirm the reboot of the AW Server.



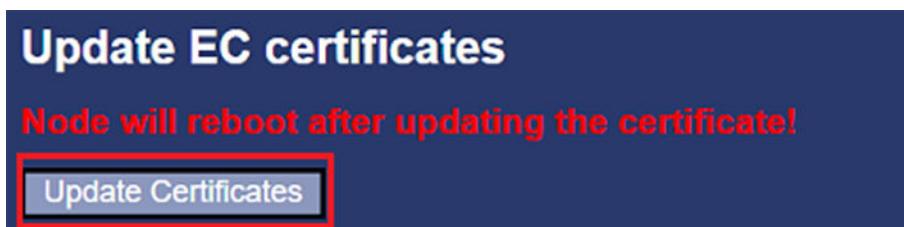
- Refresh the browser and login again into the Service Tools.



2.4.1.1.2 Renewing AW Server Web Client certificate

This section is available only if the AW Server Web Client has been installed and activated.

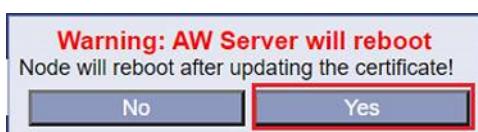
- In the *Update EC certificates* part of the page, click on **Update Certificates**.



- In the warning message that displays, confirm the removal of the previous certificate and the installation of the new certificate.



- In the warning message that displays, confirm the reboot of the AW Server.



4. Refresh the browser and login again into the Service Tools.



2.4.2 Utilities

The Administrative > Utilities options are explained in this section.

2.4.2.1 Manage Clients

This tool provides :

- the means to send a one-way broadcast message to all connected clients, and
- the capability to list all connected clients, select individual (or all) clients for disconnection, and to send a broadcast disconnection message at the disconnection action.



2.4.2.1.1 Broadcast Message Tool

This tool allows the capability to send a broadcast message to **ALL** clients connected to the current node. The pop-up message will appear on top of the client browser window. There are THREE control buttons for the message text.

Set message – this button sends whatever text is in the message box. If there is no message text in the message box, there will be no message text in the pop-up message that appears at the client – just the pop-up window with **OK** in it. The pop-up message will disappear when the **OK** is clicked on. If new clients attempt to login while a message is in send (set) state, the pop-up message will appear to the new user at their login screen when they click LOGIN. It will disappear when they click OK on the message and login will proceed. **The message displays every time a user logs in, not just one time.**

Query message – This button will display the current message text that is set-up to send. If you have sent a message, and now start to edit the text to express a different message, but then want to go back to the original message – the Query message button will recall the message in this case.

Clear message – This button will clear the message text field. The Query button will not bring it back. However, it is important to remember to CLEAR your message texts after sending them – if you do not want the same message sent again when you did not intent it to be sent again.

NOTE

To send a message to all clients in a cluster, you must connect to each server node of the cluster and resend it.

2.4.2.1.2 Manage (disconnect) Clients

This tool will list the currently connected clients. There are TWO buttons used to control this tool.

Refresh - Use this button often! There may be a certain amount of latency in the real-time ability of the tool to list current clients. The refresh button may at time take a moment or two to update.

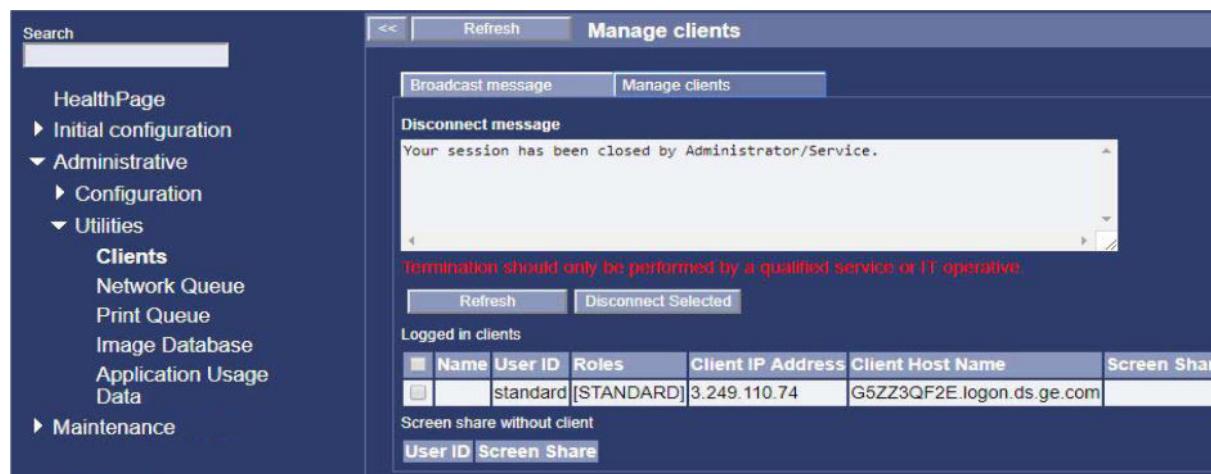
Disconnect Selected — This button will disconnect listed clients if they are selected in the selection box at the left of the list. To select ALL the listed clients — click on the box at the left of the Name heading.

NOTE

When client data cannot be retrieved for a particular client, the client list contains a row with "Unknown" labels. Refresh is needed to try to get the detailed data retrieved from the client.

NOTE

If any of the clients are sharing their screen (see [3.3.4 Troubleshooting with Screen Sharing on page 147](#) for details), there will be a link displayed under the "Screen Share" field. (Screen Sharing is not available in Full or Seamless integration and Secured for RMF mode).



As you can see, this tool allows selective disconnection of individual clients. This could be useful in situations where only one or a few clients are having issues, and you want to have then retry without interrupting the other normally functioning client connections. Unfortunately, the broadcast message tool does not allow individual message broadcasts. So, be aware of the capabilities, and word your messages accordingly.

The final element of the Disconnect tool is the message text field. This message will get sent (set) when the Disconnect Selected button is clicked and will pop-up on top of the client browser — use this to inform users that they will be disconnected, and what actions to take, for instance save open exam series. Ensure that you write the message in the language(s) understood by users.

The “default” message shown in the screen-shot above is the message that will be sent if you do not edit it or delete it. This is to try and ensure that “something” is sent when a deliberate disconnection is initiated.

NOTE

If you are intervening on a cluster and do not see a specific known client, connect to each node of the cluster in turn until you find the one to which it is logged on.

2.4.2.2 DICOM Network Queue and DICOM Print queue

There is no DICOM queue access from the client browser — only in the Service Tools — ADMIN can access this tool. The tool is linked to the **HealthPage Server Configuration status**. Very large jobs might be in the queue for a few minutes or hours — depending on the network, but unless there is a failure or pause — there will not be any persistent queue listing or status.

Access the DICOM Network and DICOM Print queues through **Administrative / Utilities** menu

Figure 2-3 SERVICE TOOLS DICOM NETWORK QUEUE

E/S/I	Type	Status	Progress	Date	Source	Target
2474/20068	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 14:47:57 GMT+200 2010	Local DB	cse-msp-server
2474/20068	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 08:16:30 GMT+200 2010	Local DB	cse-msp-server
2474/20067	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 08:15:35 GMT+200 2010	Local DB	cse-msp-server
101/20101	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 10:50:29 GMT+200 2010	Local DB	cse-msp-server
2474/20067	push	Failed	push failed: cse-msp-server could not perfor...	Fri May 07 09:23:23 GMT+200 2010	Local DB	cse-msp-server
2474/20068	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 16:22:16 GMT+200 2010	Local DB	cse-msp-server
2474/20067	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 10:15:18 GMT+200 2010	Local DB	cse-msp-server
258/20108	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 19:06:41 GMT+200 2010	Local DB	cse-msp-server
2474/20067	push	Failed	push failed: cse-msp-server could not perfor...	Thu May 06 16:18:48 GMT+200 2010	Local DB	cse-msp-server

Figure 2-4 SERVICE TOOLS DICOM PRINT QUEUE

Description	Destination	User	Status	Submitted On	Type	Identifier
AVDaorta02	DF500	john	Active	28-Jun-2014 20:51:51	DICOM	1

Be sure to use the **Refresh** button often.

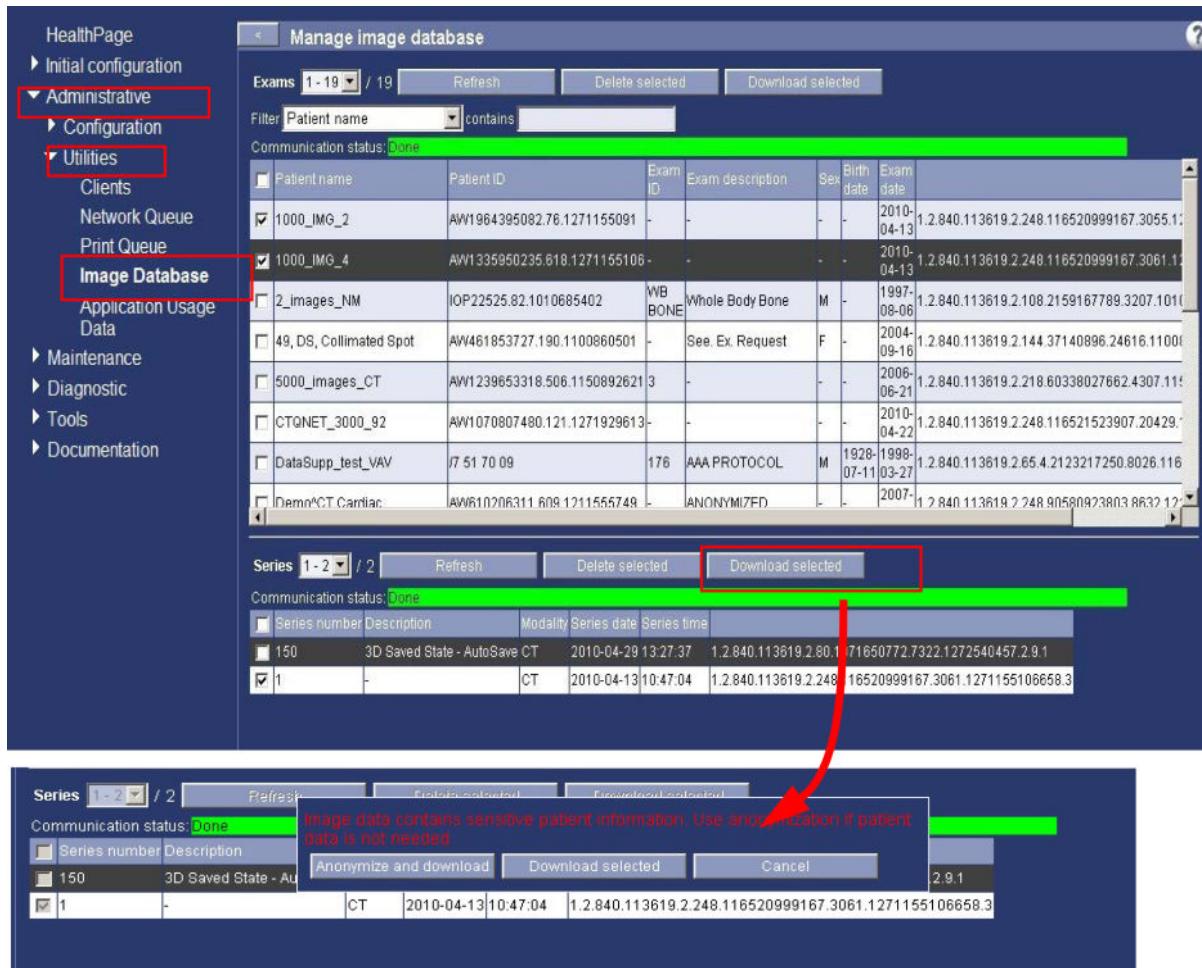
One typical usage scenario might be when the HealthPage status indicates a failed job or jobs. Use this tool as the next step in discovering what is happening, and to possibly **Pause – Retry – Resume – Cancel** the job. Also, use the listing, and the **Show History & Show Details** button(s) to discover more information about the current job, or the history of other completed jobs...

NOTE

If you are intervening on a cluster and do not see a particular failed job, connect to each node of the cluster in turn until you find the one to which it is logged on.

2.4.2.3 Image Database

This is the tool that is used to **MANAGE** the server's image database, and to **anonymize data for extraction**, and service analysis. Access the **Image Database** through **Administrative / Utilities** menu. When started, a message displayed in yellow informs you that the database is queried prior to display the exams

Figure 2-5 SERVICE TOOLS IMAGE DATABASE

The Image Database tool is presented in **THREE** logical viewing panes - which correspond to the **EXAM** level, the **SERIES** level, and the **IMAGE** level.

Data can be selected using the **check boxes** on the left-hand side of the viewing panes.

Be sure to use the **Refresh** button to make sure the display is current.

There is a "**Communication status**" heading above each section in the upper left. This will indicate if the listing is in process or if the listing is "**Done**."

There is a **pull-down** in the upper left-hand corner of each section. This will have a designation indication 1 through the total number of exams, series, or images available for viewing — so you do not have to scroll through the entire list to know how many total entries there are.

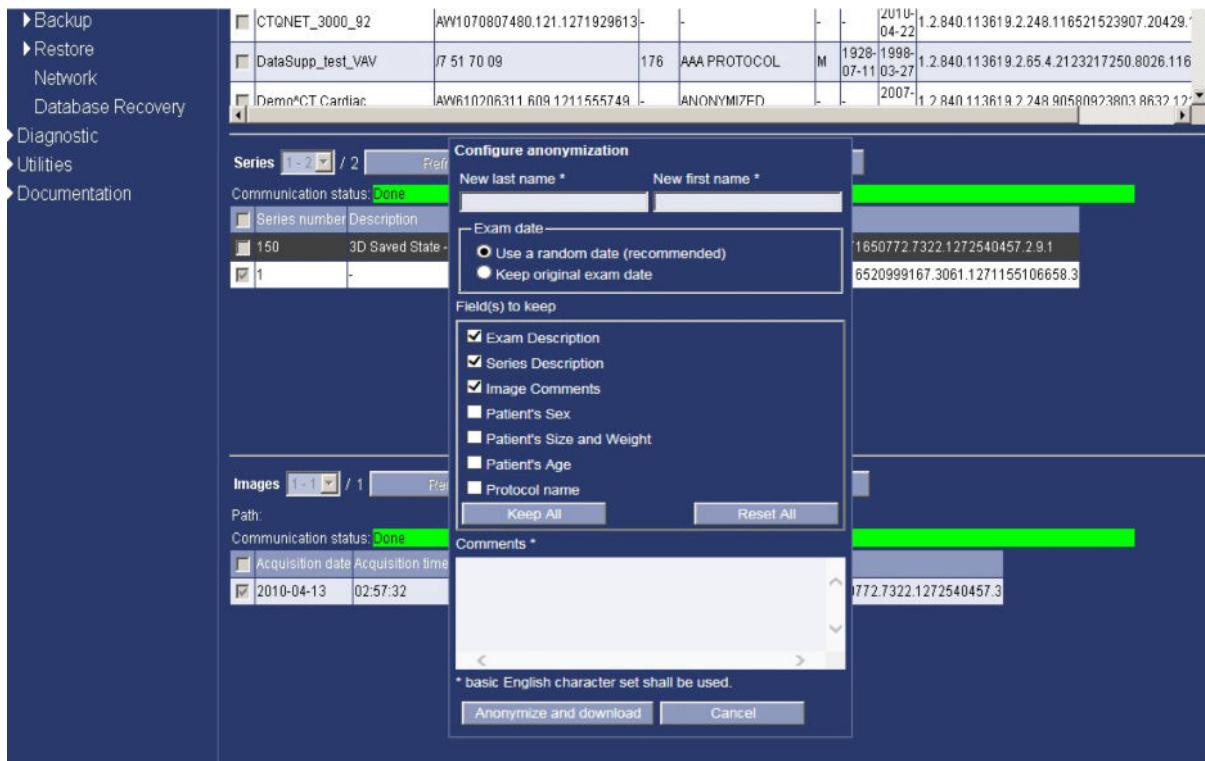
Use the **Delete selected** button to **manually manage the size of the image database** if the auto-delete function is not used, and it becomes necessary to remove data.

There is an **Anonymize and download** button pop-up menu when selecting for download. Use this tool to anonymize data for extraction and off-site analysis or use. You can select data at the **Exam**, **Series**, or **Image level**.

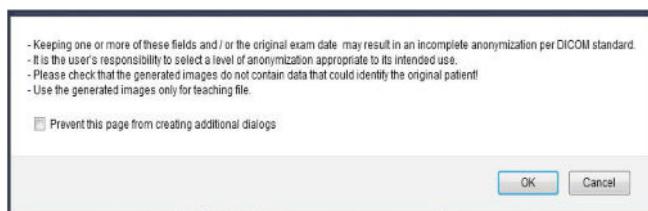
NOTE

Known limitation: when using the filtering function in this menu, do not enter text that contains the "_" character as it is not correctly handled by the filter. "_" is considered to represent any character so the filter will return too many results.

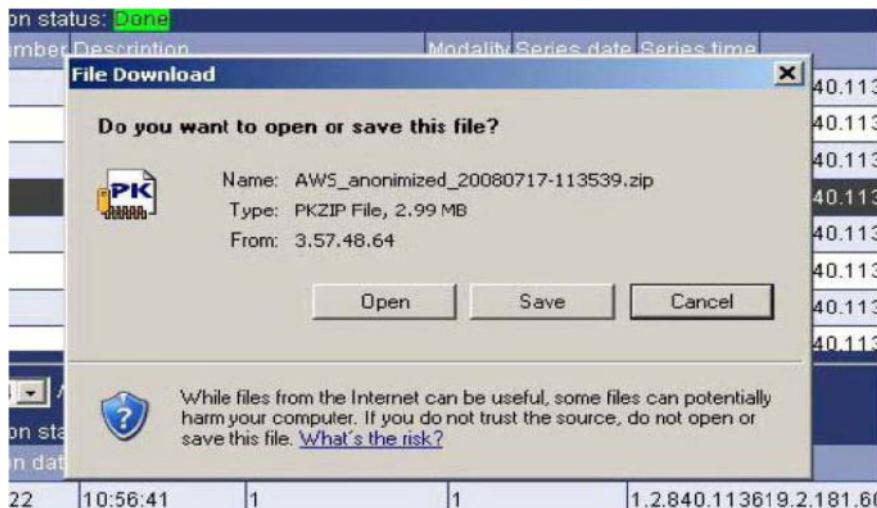
When the **Anonymize and download** button is clicked, the *Configure Anonymization* screen pops-up, in order to select the nature of the patient's attributes to be downloaded.

Figure 2-6 CONFIGURE ANONYMIZATION

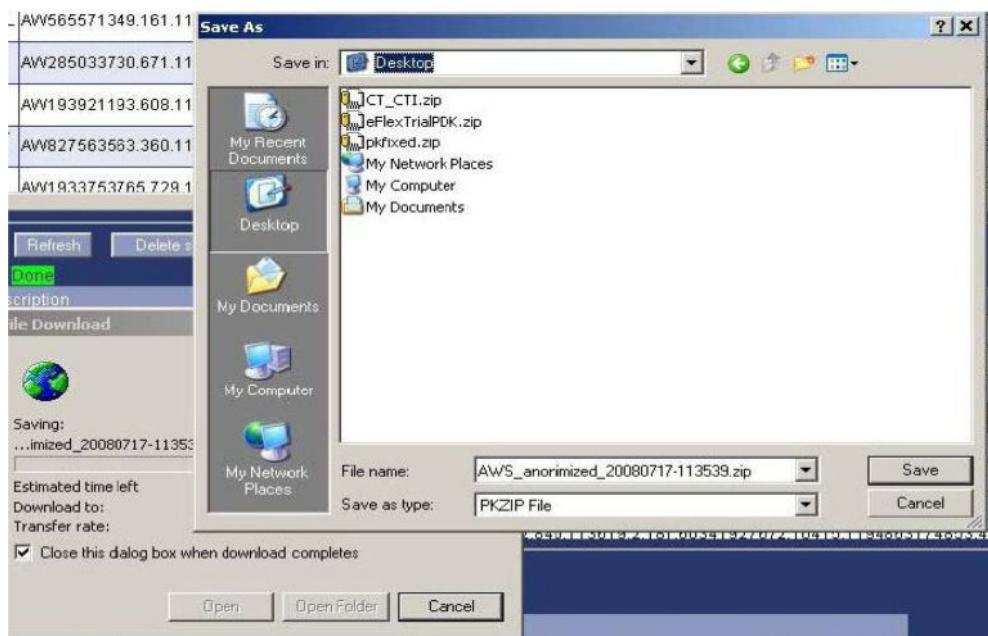
- Select whether you will keep the original exam date or use a random date (default and recommended setting).
- Select the patient's attributes that you want to keep for download.
- After selecting the patient's attributes to be downloaded, click on **Anonymize and download** button. Depending on the selection you made before (keep original date or not), you will get one of the following confirmation window pop-up. Read the message carefully, then click **OK** to accept:



- Clicking **OK**, the next pop-up (or equivalent, depending on the Internet navigator type or version) will ask what you want to do with the file — **open** it or **save** it?

Figure 2-7 ANONYMIZE AND DOWNLOAD SELECTED SAVE FILE

- For the purposes of extracting data for analysis, the intent is to **Save** the file. After clicking on **Save**, the location can be selected as to where to save the file.
- If you are connected to the Service Tools via the "**local**" intranet, you will be able to select a location on your PC.
- If you are connected via InSite (version prior to AW Server 3.2 Ext. 4.2), you will be locked into selecting a location on the GEHC InSite back-office server.

Figure 2-8 ANONYMIZE AND DOWNLOAD SELECTED SAVE FILE LOCATION

- The file that is saved is a ZIP file named similar to this example -



- In this example, the data was selected at the series level. So, the file contains the images in that particular series.

Figure 2-9 EXAMPLE ZIP FILE CONTENTS

	Name	Size	Comp Size	Type	Modified	Ratio	Folder
IOP.0	139,216	58,028	0 File	07/17/2008 11:35 AM	58.4%	anonymized_20080717-113539/	
IOP.1	139,214	66,341	1 File	07/17/2008 11:35 AM	52.4%	anonymized_20080717-113539/	
IOP.2	139,214	68,827	2 File	07/17/2008 11:35 AM	50.6%	anonymized_20080717-113539/	
IOP.3	139,214	69,634	3 File	07/17/2008 11:35 AM	50.0%	anonymized_20080717-113539/	
IOP.4	139,212	76,686	4 File	07/17/2008 11:35 AM	45.0%	anonymized_20080717-113539/	
IOP.5	139,212	74,668	5 File	07/17/2008 11:35 AM	46.4%	anonymized_20080717-113539/	
IOP.6	139,212	72,632	6 File	07/17/2008 11:35 AM	47.9%	anonymized_20080717-113539/	
IOP.7	139,212	69,324	7 File	07/17/2008 11:35 AM	50.3%	anonymized_20080717-113539/	
IOP.8	139,212	67,692	8 File	07/17/2008 11:35 AM	51.4%	anonymized_20080717-113539/	
IOP.9	139,212	63,476	9 File	07/17/2008 11:35 AM	54.5%	anonymized_20080717-113539/	
IOP.10	139,212	62,983	10 File	07/17/2008 11:35 AM	54.8%	anonymized_20080717-113539/	
IOP.11	139,216	69,412	11 File	07/17/2008 11:35 AM	50.2%	anonymized_20080717-113539/	
IOP.12	139,214	69,526	12 File	07/17/2008 11:35 AM	50.1%	anonymized_20080717-113539/	
IOP.13	139,216	69,191	13 File	07/17/2008 11:35 AM	50.3%	anonymized_20080717-113539/	
IOP.14	139,216	69,887	14 File	07/17/2008 11:35 AM	49.8%	anonymized_20080717-113539/	
IOP.15	139,216	68,383	15 File	07/17/2008 11:35 AM	50.9%	anonymized_20080717-113539/	
IOP.16	139,216	65,792	16 File	07/17/2008 11:35 AM	52.8%	anonymized_20080717-113539/	
IOP.17	139,216	64,221	17 File	07/17/2008 11:35 AM	53.9%	anonymized_20080717-113539/	
IOP.18	139,216	62,847	18 File	07/17/2008 11:35 AM	54.9%	anonymized_20080717-113539/	
IOP.19	139,216	59,435	19 File	07/17/2008 11:35 AM	57.4%	anonymized_20080717-113539/	
IOP.20	139,216	58,040	20 File	07/17/2008 11:35 AM	58.4%	anonymized_20080717-113539/	
IOP.21	139,216	52,701	21 File	07/17/2008 11:35 AM	62.2%	anonymized_20080717-113539/	
IOP.22	139,216	45,750	22 File	07/17/2008 11:35 AM	67.2%	anonymized_20080717-113539/	
IOP.23	139,212	78,696	23 File	07/17/2008 11:35 AM	43.5%	anonymized_20080717-113539/	
IOP.24	139,212	84,048	24 File	07/17/2008 11:35 AM	39.7%	anonymized_20080717-113539/	
IOP.25	139,210	83,538	25 File	07/17/2008 11:35 AM	40.0%	anonymized_20080717-113539/	
IOP.26	139,212	83,289	26 File	07/17/2008 11:35 AM	40.2%	anonymized_20080717-113539/	
IOP.27	139,212	83,595	27 File	07/17/2008 11:35 AM	40.0%	anonymized_20080717-113539/	
IOP.28	139,214	82,249	28 File	07/17/2008 11:35 AM	41.0%	anonymized_20080717-113539/	
IOP.29	139,210	82,522	29 File	07/17/2008 11:35 AM	40.8%	anonymized_20080717-113539/	
IOP.30	139,210	82,648	30 File	07/17/2008 11:35 AM	40.7%	anonymized_20080717-113539/	
IOP.31	139,210	83,435	31 File	07/17/2008 11:35 AM	40.1%	anonymized_20080717-113539/	
IOP.32	139,210	82,669	32 File	07/17/2008 11:35 AM	40.7%	anonymized_20080717-113539/	
IOP.33	139,212	82,014	33 File	07/17/2008 11:35 AM	41.1%	anonymized_20080717-113539/	
IOP.34	139,210	81,573	34 File	07/17/2008 11:35 AM	41.5%	anonymized_20080717-113539/	
IOP.35	139,212	80,337	35 File	07/17/2008 11:35 AM	42.3%	anonymized_20080717-113539/	
IOP.36	139,212	80,559	36 File	07/17/2008 11:35 AM	42.2%	anonymized_20080717-113539/	
IOP.37	139,212	79,515	37 File	07/17/2008 11:35 AM	42.9%	anonymized_20080717-113539/	
IOP.38	139,216	67,246	38 File	07/17/2008 11:35 AM	51.7%	anonymized_20080717-113539/	
IOP.39	139,216	61,783	39 File	07/17/2008 11:35 AM	55.7%	anonymized_20080717-113539/	
IOP.40	139,216	65,602	40 File	07/17/2008 11:35 AM	52.9%	anonymized_20080717-113539/	
IOP.41	139,216	65,424	41 File	07/17/2008 11:35 AM	53.1%	anonymized_20080717-113539/	
IOP.42	139,214	69,356	42 File	07/17/2008 11:35 AM	50.2%	anonymized_20080717-113539/	
IOP.43	139,214	70,562	43 File	07/17/2008 11:35 AM	49.4%	anonymized_20080717-113539/	

Files Comment Statistics SFX/Options Log

New creates a .ZIP file; Open accesses an existing file. 44 files, 5981 KB 1 files, 135 KB

- Once the files are extracted from the ZIP file, they can be viewed with a DICOM image viewer application. See Chapter 3 [3.4.5.9 Troubleshooting Images on page 197](#).

NOTE

These file extraction and manipulation examples are based on a "Windows" based implementation of the ZIP file. The corresponding Linux or Unix ZIP file characteristics and implementations will produce the same DICOM-viewer-ready-file results.

NOTE

In the case of Seamless Integration of physical AW Server with a PACS image database (no DAS), there is a small local image partition which is used to stock images processed by the AW Server prior to pushing them to the PACS.

2.4.2.4 Application Usage Data

2.4.2.4.1 Overview

The AUM feature, also known as Software Metering, allows you to track application usage for compatible applications. Data is compiled in a database by EAT (Enterprise Audit Trail).

This data is also available for analysis on the server, from the Service Tools menu **Administrative > Utilities > Application Usage Data**.

The tool lets you consult the number of times each application has been used on exams. Results contains information about date, users, and applications.

As well as basic site/system configuration, the following information about software application usage is captured:

- User id (e.g. sdc, foobar)
- Study UID
- Timestamp
- Application license name
- Application Pretty Name

NOTE

If the given application is launched several times with the same study, only one usage is counted.

To display application usage for a given period:

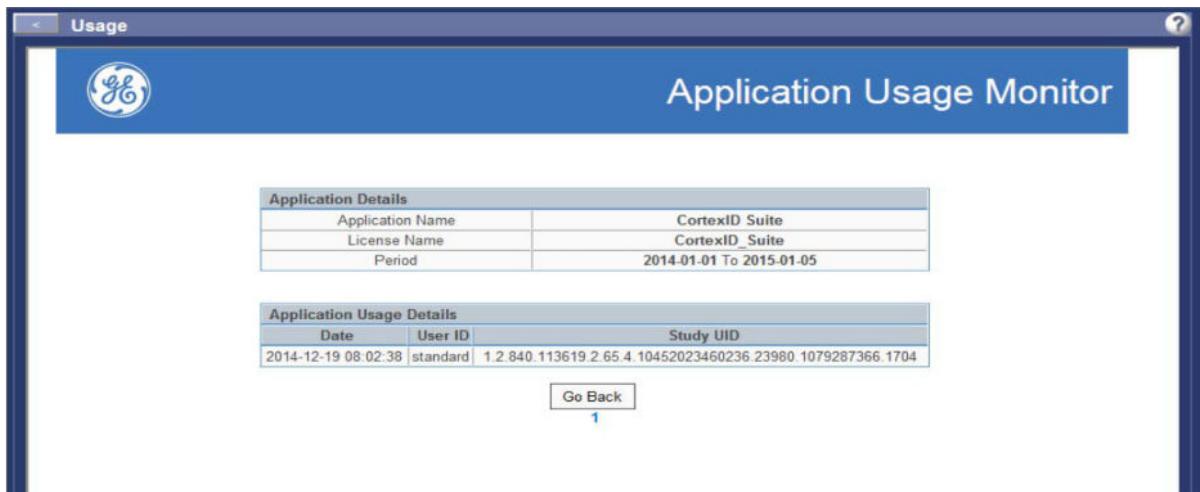
- Login to the server's Service Tools with any Admin / user account.
- From the menu bar, select **Administrative > Utilities > Application Usage Data**.
- Specify a period Start and End using the calendar widget and click **Display**.

The screenshot shows the 'Usage' section of the Service Tools interface. On the left, there's a navigation sidebar with links like 'HealthPage', 'Initial configuration', 'Administrative', 'Configuration' (with sub-links for DICOM Hosts, Users (EA3), Client Timeout, Floating License, Preprocessing, and End Of Review), 'Utilities' (with sub-links for Clients, Network Queue, Image Database, and Application Usage Data), and 'Application Usage Data'. The main area has a title 'Application Usage Monitor' and a sub-section 'Please select a period' with 'Start' and 'End' date pickers set to '2014-12-17'. Below this is a table titled 'Application Usage Details of applications between 2014-12-17 To 2014-12-17'.

Applications	Count	Details
Volume_Viewer	10	Click here
MR_VesselQ_Xpress	1	Click here
OneQuant	1	Click here
Integrated_Registration	2	Click here

A list of applications used during that period displays, and the number of times each was launched.

To view full details for an application, click the corresponding **Click here** link.



To return to the previous screen, click the **Go Back** button.

NOTE

Detailed application usage data is only available for the current year and previous year.

To display summary data for a previous year:

- Select the View History icon on the Usage screen.
- Select an available year from the **Year** drop-down menu and click **Display**.

The listing shows a list of applications and the number of times they were launched during the selected year.

The screenshot shows the 'Application Usage Monitor' window. At the top, there's a blue header bar with the GE logo on the left and the title 'Application Usage Monitor' on the right. Below the header, there's a message 'Select a year to view its application usage history' and a dropdown menu set to '2010'. Below the dropdown are 'Display' and 'Go Back' buttons. At the bottom, there's a table titled 'Application Usage Summary' with four columns: Application Name, License Key String, Count, and Year. The table contains two rows: one for 'App14061' with 'lic_App14061' as the license key, '1' as the count, and '2010' as the year; and another for 'GERemoteUpdate' with 'lic_App12926' as the license key, '1' as the count, and '2010' as the year.

To return to the previous screen, click the **Go Back** button.

NOTE

Application Usage Data is not lost after a Database Recovery, however this data is lost after a Load From Cold (reinstallation of OS + platform). This data is not part of the system configuration backup.

2.5 Tools Menu

2.5.1 Terminal

2.5.1.1 How to use the Terminal

This tool opens a command-line terminal to the AW Server. It gives the user local command-line access from a remote location via the Service Tools web interface.

Terminal allows the user to do such things as:

- Examine logs manually,
- Execute scripts manually,
- Analyze the file-system and operating system environment manually.
- Enter commands to the AW Server, such as when installing or configuring the server.

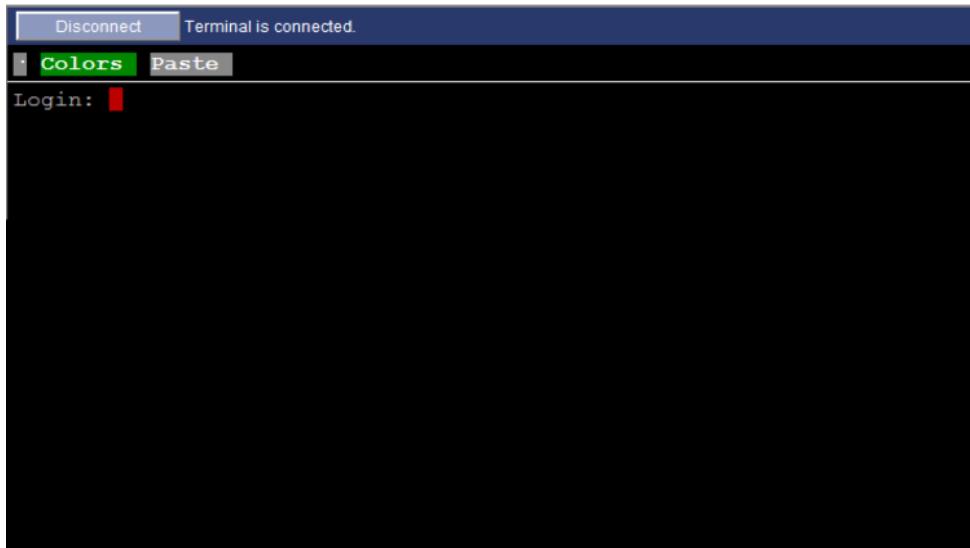
Terminal Tool Usage — allows the user to enter commands to the AW Server, such as when installing or configuring the server.

- From the text menu on the left side of the Service Tools page, click the ► arrow next to "**Tools**" to expand the Tools menu. When the next menu level displays, click "**Terminal**." The Terminal page will display.

Figure 2-10 TERMINAL PAGE (SERVICE TOOLS) -- CONNECT



- Click the "**New modal Terminal**" button to open a terminal in a new, separate window. You can go back to the initial tab and navigate in the Service Tools, it will not close the Terminal connection in the separate tab.

Figure 2-11 TERMINAL SESSION WINDOW (SERVICE TOOLS)

- At the “Login:” prompt, type **root**, then press **<Enter>**.
- At the “Password:” prompt, type in the default root password **<Enter>** (unless it has been changed to something else — see chapter 9, [A.6 Password Change on page 484](#)).

NOTE

For security purposes, Terminal does not display any characters while you type the password.

- You are now logged into the AW Server. You can send commands to the server via the command line interface. i.e.: **conf <Enter>** to display the AWS configuration parameters
- When you have finished using Terminal, type **Logout** to disconnect from the AW Server.

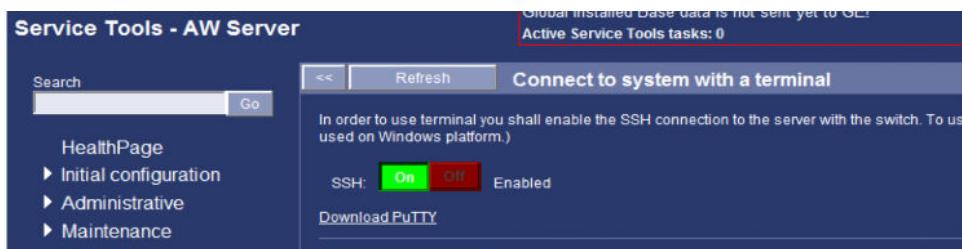
2.5.1.2 Using an ssh client instead of Terminal

The Terminal included in the Service Tools has several limitations: no scrollbar, difficulties to use special character like pipe “|”. An alternative is to temporarily enable ssh access, using the interface from the Service Tools.

This procedure can also be used to enable ssh access for AW Servers managed by GEHC IT Remote Service.

To enable ssh:

- Go to the Service Tools page **Tools > Terminal**.
- In the upper part of the page, check the line indicating the SSH status.
- If SSH is disabled, click on the “On” green switch to enable SSH. A success message displays and SSH status is “Enabled”.

**To disable ssh:**

- Go to the Service Tools page **Tools > Terminal**
- In the upper part of the page, check the line indicating the SSH status.

- If SSH is enabled, click on the “Off” red switch to disable SSH. A success message will display and SSH status is Disabled.

Once SSH is enabled, use an SSH client to connect to the AW Server. The SSH client “putty” is included in the AW Server and can be downloaded from the Service Tools page **Tools > Terminal**. Click on the link **Download PuTTY** to save the file on your computer, then double click on putty.exe to launch the SSH client. Use the IP address of the AW Server to connect.

NOTE

If using a remote connection (Insite/RSvP), use the SSH connectivity tool or the Terminal tool in FFA.

2.5.2 File Transfer Tool

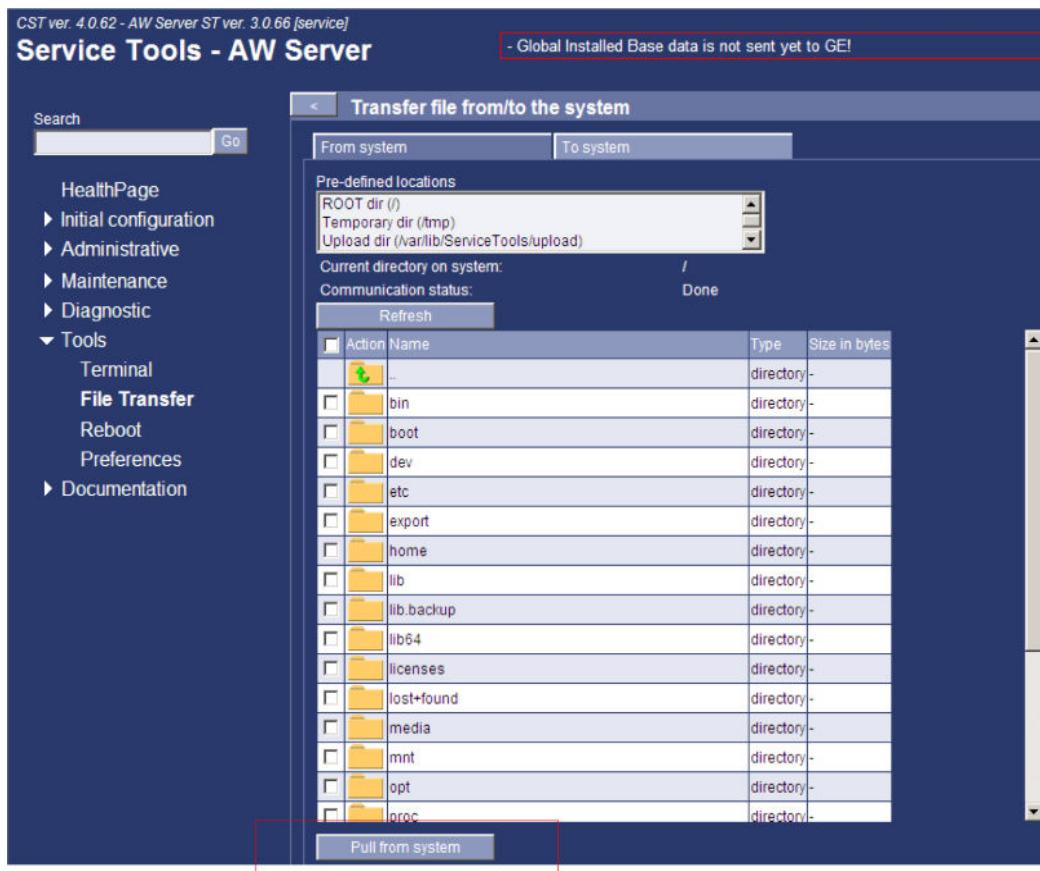
This tool is used to transfer files to and from the AW Server (for example, to install application ISO files). There is a maximum size when downloading from system. To download bigger sizes, consider using the FFA File Transfer tool.

There are two options in File Transfer tool: pull files **From System** (server) and push files **To System**. The **From System** is the default tab when you start the File Transfer tool.

2.5.2.1 How to Start the File Transfer Tool

- From the text menu in the left column of the Service Tools page, click  to select **Tools**.
- When the Tools menu expands, click on **File Transfer**.

The File Transfer page should display



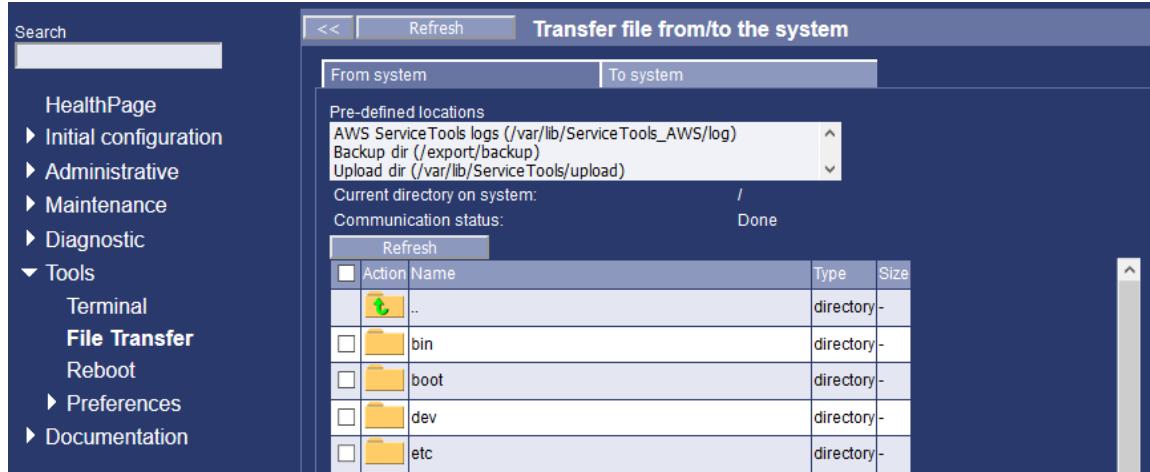
- There are two pages in the File Transfer tool.

1. The default page - which is displayed when the File Transfer tool is started - this is the "From Server" page. The "From server" page can also be used to see (browse) which files and subdirectories are contained in each directory on the AW Server.
2. The other File Transfer page is the "**To Server**" page - which is used to send files to the AW Server.

2.5.2.2 File Transfer from Server

- From the File Transfer page, select the "**From System**" tab. The File Transfer "From server" page will display.

Figure 2-12 "FROM SYSTEM" TAB



2.5.2.3 How to use the File Transfer "From Server" Tool – Basic Steps

There are three basic steps to using the File Transfer "From server" tool:

1. Display the file or directory to be transferred from the pre-defined location
2. Click on its selection box
3. Click the **Pull from Server** button.

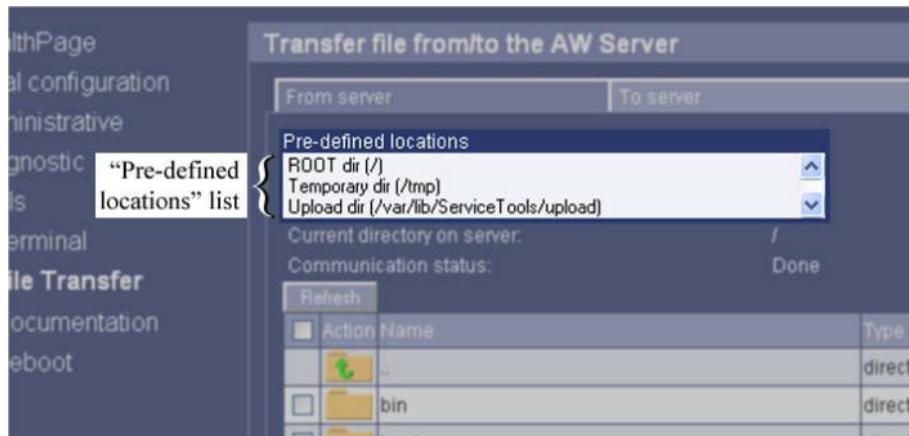
2.5.2.4 Selecting the Directory to View

You can select the listed directory two ways: Either by using the "Pre-defined locations" list - or by clicking directly on a directory in the directory contents list.

NOTE

The default directory is the root directory (i.e., the highest level).

1. "**Pre-defined locations**" list - provides a shortcut to a list of commonly used directories, as in the figure. Each listing provides the complete path for that directory location. To list the contents of one of these directories, click on the location you want, and a list of the contents will display in the directory list window below.

Figure 2-13 PRE-DEFINED LOCATIONS LIST (EXAMPLE)**NOTE**

If you select one of the Pre-defined locations to display, then change the list by clicking on a directory in the directory contents list, the path shown in the Pre-defined locations does NOT change to reflect the new directory you have selected. The list of Pre-defined locations always remains the same.

NOTE

You may have to scroll down to view the entire Pre-defined locations list.

- You can click on a listed directory to display its contents (you can click on either the icon or the directory name), but clicking on a file name doesn't do anything, because there is no next-lower level to list.

2. **Selecting a directory from the directory contents list** - To transfer a file from a location not listed in the Pre-defined locations list, you can use the directory contents list to select individual directories for viewing. To view the contents of a directory in the list (i.e., a directory that is one level down from the displayed directory), click the icon next to the name of the directory.

To view the contents of the next higher-level directory, click the icon at the top of the directory list. Each time a directory is selected, the File Transfer page will list the contents of that directory.

NOTE

Clicking the icon while in the root directory does not do anything, because there is no higher level to go to.

NOTE

Allow a few seconds for the list of the directory's contents to display.

- To select an AW Server file (example)

For example, if you wanted to select a file named "file.abc" (Note: this is not a real file.) - for which the path is "/tmp/export/home/file.abc".

From the root directory (the default directory that File Transfer starts out in when you first launch it):

- a. Click the "tmp" directory to list its contents.
- b. When that directory displays, click the "export" directory.
- c. When that directory displays, click the "home" directory. You are now at the last directory in the path. The file "file.abc" will display in the directory contents list. Click its selection box () to select it for transfer.

- d. You can select more than one file.
- To select an AW Server directory (example)

The process for transferring a directory is similar to transferring a file, except that you set File Transfer tool to display the directory one level up.

For example, if you wanted to transfer the directory "home" from the previous example, do the following:

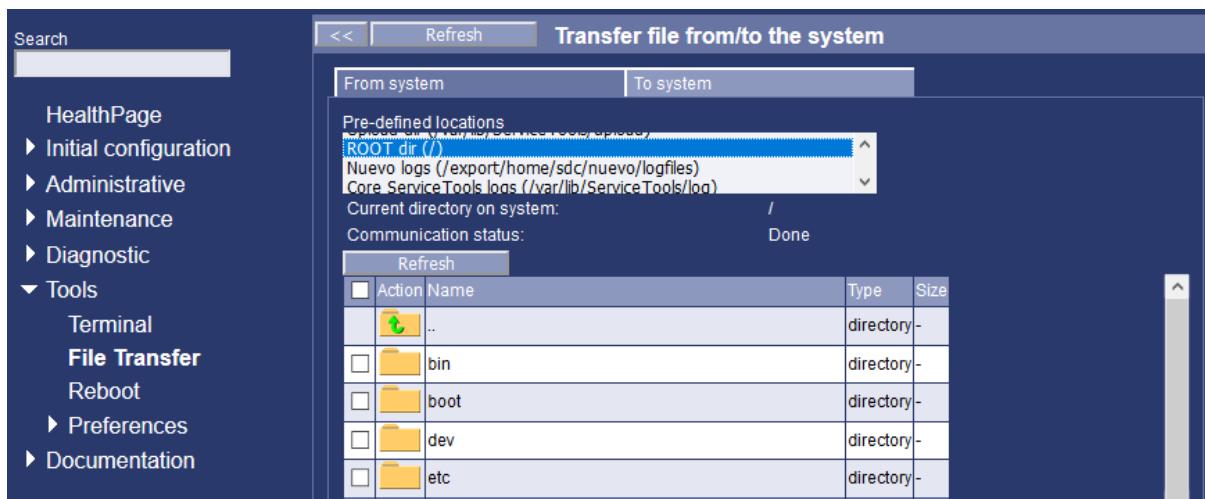
The path is "/tmp/export/home/". But because you want to transfer the "/home/" directory, you will need to display the "/tmp/export/" directory, because that is the directory that contains the "/home/" directory. So, from the root directory (the default directory that File Transfer starts out in when you first launch it), you would do the following:

- a. Click the "tmp" directory to list its contents.
- b. When that directory displays, click the "export" directory. Do NOT go down one more level.
- c. The "/home/" directory is included in the directory contents list. Click its selection box () to select it for transfer.
- d. You can select more than one directory, or a combination of files and directories.

- Location or path of current directory

The location or path of the current directory is displayed as shown in the figure. Each time a different directory is selected, this display will change to show the path of the directory that is displayed.

Figure 2-14 PATH OF CURRENT DIRECTORY



2.5.2.5 Communication Status Message

This status message indicates whether or not the most recently selected directory was successfully retrieved from the AW Server.

NOTE

The Communication status message displays only for a very short time.

When a directory is selected for display, the status message, "**Communicating with server**" is displayed on a yellow background. This message displays while the File Transfer tool is retrieving the contents of the selected directory.

When the directory is successfully retrieved, the status message, "**Done**" is displayed.

2.5.2.6 Directory Contents List

The files and directories contained within a directory are shown in the directory contents list shown in the figure.

NOTE

Directories below the level of the displayed directory are not listed. The list shows only what is contained one level down from the selected directory. (In other words, it lists only directories, not "subdirectories".) To see what is contained at the next-lower level in a directory, click on that directory to display a list of its contents.

- **Refresh button** - Click the "Refresh" button to update the list of the contents of the current directory. You can do this to view additional files or directories that have been added to the current directory since you first selected it.

- **Selecting the AW Server files to transfer:**

Select each file or directory that you want to transfer by clicking on the "check box" (selection box) on the left side of the column next to the item name. You can check more than one item.

A check mark will appear in the selection box () when you click it, indicating that you have selected that item to transfer. To de-select the item, click the box again. In the example figure, the first three files in the directory are selected.

Figure 2-15 THREE SELECTED FILES (EXAMPLE)

Action	Name	Type	Size in bytes
<input type="checkbox"/>	..	directory	-
<input checked="" type="checkbox"/>	dbxd.log	file	0
<input checked="" type="checkbox"/>	er.console.out	file	121
<input checked="" type="checkbox"/>	eventRouter.log.0	file	44002
<input type="checkbox"/>	eventRouter.log.0.lck	file	0
<input type="checkbox"/>	fastLaunch.console.out	file	1067
<input type="checkbox"/>	fastLaunch.log.0	file	014

- Selecting the entire directory to transfer

To select the entire contents of a listed directory, click the selection box next to the word "Action" (at the top of the check-box column), as shown in the figure. This will select all the selection boxes at once. Click the box again to de-select the entire contents.

NOTE

Some directories can't be selected. If a listed directory doesn't have a check box next to its name, it can't be selected.

Figure 2-16 SELECTING ALL THE CONTENTS OF A DIRECTORY



2.5.2.7 Transferring AW Server Files to Another Location - Procedure

- Select the "**From server**" tab

- Select the directory to display
- Select files and/or directory to transfer by clicking the box (selection box) next to each item you want to transfer. Click a box once to select it; click it again to de-select it.
- When you have selected all the files and/or directories you want to transfer, click the **Pull from System** button at the bottom of the page.
- A popup box might display a note about the file size. If it does, click “**OK**.”
- The browser will ask if you want to open or save the file. Click “**Save to Disk**.”
- The browser will display the file-naming window. Use the existing file name, or choose a different one if you want. Select the folder you want to save the file to, then click the “**Save**” button.
- The files will transfer to the specified location ...

Verifying the file transfer to the client:

To verify that the file or directory did transfer, use Windows Explorer or a similar program on the destination system to view the contents of the directory that you sent the file(s) to.

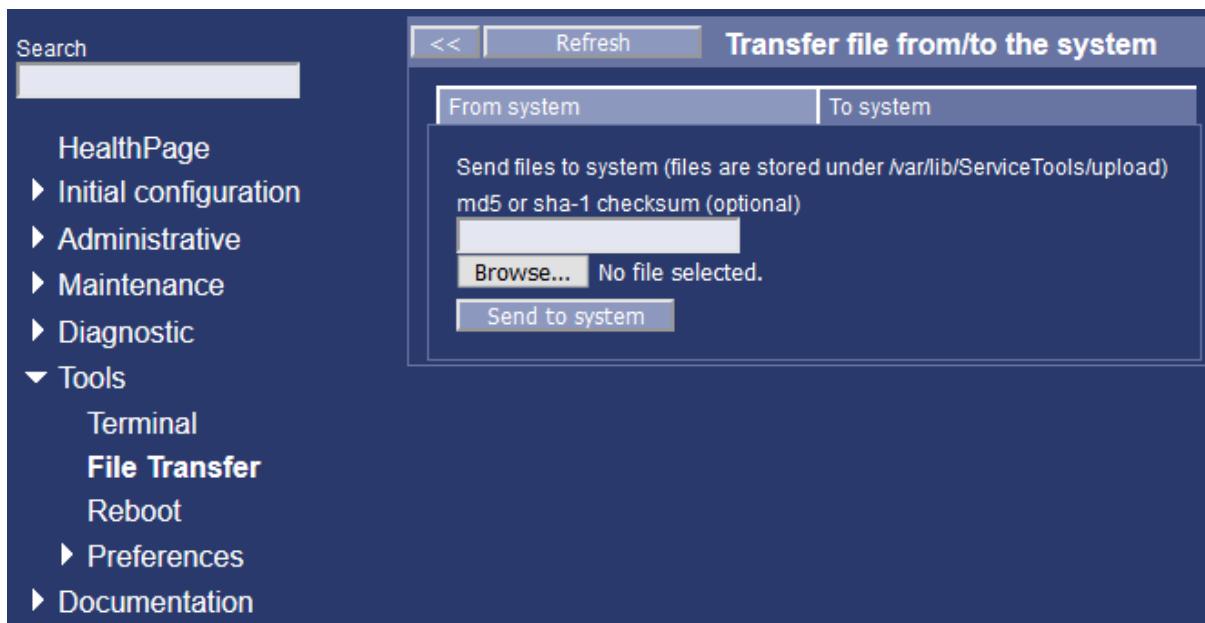
NOTICE

To retrieve data from a sites to assist issue analysis, use the FFA File Transfer tool.

2.5.2.8 Transferring a File from the Client to the AW Server

From the File Transfer main page, click the **To system** tab as shown in the figure. The File Transfer “To system” page will display.

Figure 2-17 FILE TRANSFER "TO SYSTEM" PAGE



- Selecting a file to transfer to the Server

Click the “**Browse...**” button (as shown in the figure) to look for files on your computer — the computer you are accessing the AW Server Service Tools from.

NOTE

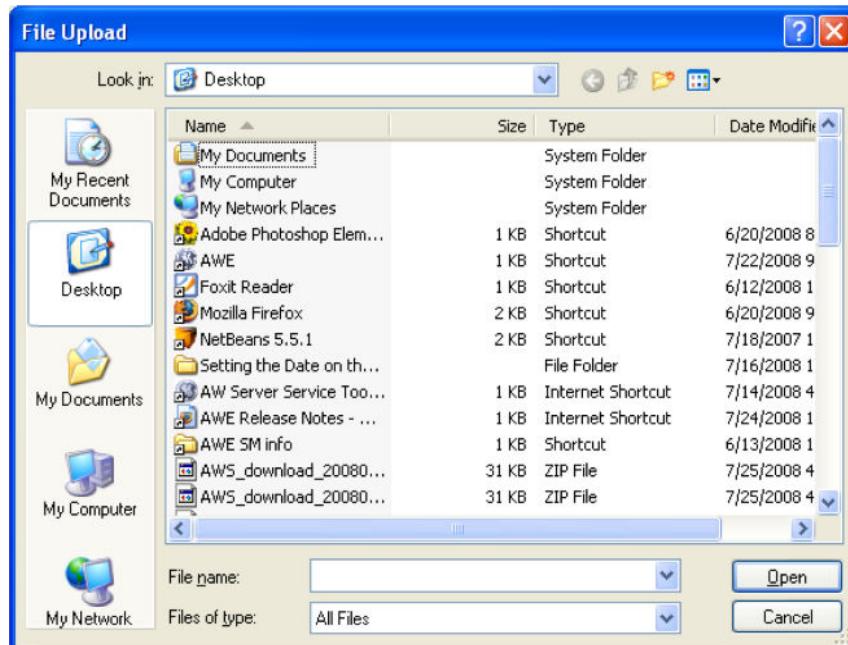
If you already know the exact file name and path, you can enter it into the box next to the “**Browse...**” button.

Your browser will display a popup window similar to the one shown in the figure.

NOTICE

This transfer procedure shall NOT be used from FFA as it is NOT compliant with service procedures.

Figure 2-18 POPUP WINDOW FOR FILE UPLOAD (EXAMPLE)



NOTE

This figure is provided only as an example. The popup window will be somewhat different depending on which browser you are using (e.g., Internet Explorer®, etc.), but the procedure will be very similar.

- Transferring the file to the server

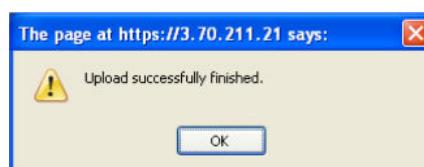
Find the file you want to transfer to the server, click the file name once to put it into the "**File name**" box, then click the "**Open**" button to start the file transfer. Or you can click the file name twice, which will start transferring the file and will close the File Upload box automatically.

The file will transfer to the server and will be stored in the server's Upload directory `/var/lib/ServiceTools/upload/`

A progress bar will inform you of the progress of the upload.

A popup box will confirm that the file transferred successfully to the AW Server, as shown in the figure.

Figure 2-19 FILE TRANSFER CONFIRMATION POPUP BOX (EXAMPLE)



- Verifying the file transfer to the server

To verify that the file did transfer to the server, go to the "**From server**" page. In the list of "Pre-defined locations", select "Upload dir `/var/lib/ServiceTools/upload/`." A list of the contents of the Upload directory will display. Any files you transferred to the server should be listed there.

2.5.3 Shutdown / Reboot

NOTICE

Shutting down or rebooting the AW Server CAN CAUSE DATA LOSS. Ensure the following before proceeding:

- All active sessions are closed and all users are disconnected.
- A database rebuild is not in progress. (To check whether database recovery is active, use the **Utilities > Terminal** option from the AWS Service Tools on the server, and after connecting and logging in, check whether the **restore-images.sh** script is running; for example, by typing the following command:

ps -aef | grep restore-images <Enter>

-Check the Service Tools HealthPage details for the last image database reset. If it was more than 180 days ago, the server will initiate one, when you reboot, resulting in a reboot time of up to 8 hours. DO NOT shutdown and/or reboot UNLESS YOU ARE CERTAIN that your action will not cause inadvertent client data loss or avoidable server downtime during core hours.

NOTICE

Please check the mount count and next file check date on the system HealthPage before rebooting the system. Rebooting a physical server will take a long time due to file system checks when:

- The **image partition mount count** threshold is reached,
- OR
- The **image partition next file system check date** is reached

NOTE

It is recommended that a reboot involving a File System Check is only performed when the server is not used (just before or during the weekend for example).

2.5.3.1 Using Command lines

To shutdown and/or reboot the AW Server, open a Terminal from the **Service Tools / Tools** menu, login as root and type the following command:

shutdown now <Enter>

shutdown -h 0 <Enter> (allowing grace delay for the users to save and quit before shutdown)

Alternatively, you can use the **init 0 <Enter>** or **halt <Enter>** or **poweroff <Enter>** commands to perform an immediate shutdown.

reboot <Enter>

Alternatively, you can use the **init 6 <Enter>** command to perform a reboot.

2.5.3.2 Using AWS scripts

These scripts perform the same actions as the shutdown or reboot commands available in the Service Tools, but at the same time send a message to the users connected:

- **shutdownAWS**

- **rebootAWS:** invokes `/sbin/init 6` which runs the shutdown scripts before rebooting - thus a "graceful reboot"
- **rebootAWSWF:** **forces the filesystem check** and invokes `touch /forcefsck` then **reboot** which will reboot the system and launch **fsck**.

NOTE

These are emergency scripts. It is always preferable to shutdown using the Service Tools, if possible.

2.5.3.3 Using the Reboot tool

A quick way to reboot the AW server during installation/configuration is to use the **Reboot** utility under the **Tools** menu. **The Reboot options allow the Service Tools user to immediately reboot the server remotely, with or without a File system check.**

When the AW Server is in use, prefer the Maintenance mode in order to warn the Users first, that the server will be rebooted, and to let them the necessary time to save their work.

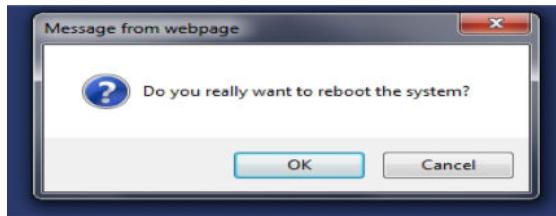


The Reboot service tool displays a message similar to the following:

*"Warning: Reboot WILL DISCONNECT ALL USERS and ANY ACTIVE SESSION DATA WILL BE LOST!
Entering Maintenance Mode first is strongly recommended."*

You have the option to ignore this message and use the Reboot tool without using the Maintenance Mode if you deem it safe - click the "**Reboot server**" button. The web browser will pop up a message asking, "Do you really want to reboot the server?" as shown in the figure. If there is any reason you do NOT want to reboot the server at this time, click "Cancel."

Figure 2-20 REBOOT REQUEST CONFIRMATION MESSAGE (EXAMPLE)



If you DO want to reboot the server immediately, click "**OK.**" The server will reboot, and the browser will pop up a message saying, "**Successfully initiated reboot.**" Click "**OK**" to close the popup.

NOTE

The users **are not** logged out upon reboot. The users receive a message that the server is going to reboot and they shall try to login after some time. Since the boot process takes a certain amount of time to complete, allow at least five minutes for the server to finish rebooting before attempting to login again. If the server doesn't respond to your login attempt, wait a few more minutes, then try logging in again.

Reboot will not cancel the Maintenance Mode. If the AW Server is in Maintenance Mode before the reboot, it will still be in Maintenance Mode after the reboot.

- If the server does not reboot, you will not be able to log back into the Service Tools. See Chapter 7, [7.8 HP Escalation and Communication Flow on page 464](#) for details of the HP iLO Service Processor, to attempt to re-try the reboot or power cycle the server.

- If the iLO **Console Redirect** is functional from your connection point, it can be used to see what is happening while using the iLO **Remote Power Control** to reboot. However, the console redirect tool may not be supported through the GEHC remote connection (InSite/RSvP).

The **Shutdown** option on the Reboot screen performs a complete system shutdown. Note that power is still applied to the server after the software has finished the graceful shutdown.

2.5.3.4 Using the Hypervisor

NOTE

Always ensure that the VMware Tools are configured, to provide a way to gracefully shutdown the guest operating system (the AW Server Virtual Machine). Refer to section [3.13.4 VMware Tools - ESXi Server Compatibility](#) on page 356 for more details.

The following can only be done on a virtual AW Server. For VMware hypervisor (ESXi):

1. Connect to the *ESXi Web Interface*.
2. Display the list of Virtual Machines.
3. Select the Virtual Machine.
4. Click on the



button to do a graceful shutdown of the AW Server Virtual Machine.

2.5.4 Preferences

NOTE

This tool is primarily intended for Standard users rather than Service or IT Admin users. However, the FE should explain to the customer IT Admin / users how to use it. The following information is provided for reference, however.

2.5.4.1 Manual Import

The **Preference Sharing Manager (PSM)** allows users to share preferences/protocols from other users, eliminating the need for each user to re-create the new preferences/protocols from colleagues.

- Select **Tools > Preferences > Manual import**

The screenshot shows the 'Preference Management' interface with the 'Manual import' tab selected. On the left, a sidebar lists various tools and documentation. The main area displays a table of preferences being imported from a user named 'alain'. The table includes columns for Application, Preference, and Status. Most entries show a 'Success' status, except for one entry for 'Viewer' which is 'Failed'.

Application	Preference	Status
Viewer		Failed
Volume Viewer	Global_userPrefs_alain	Success
Volume Viewer	MyTools_alain	Success
Filmer	CT Anglo, Runoff	
Filmer	CT/XR Runoff	
Filmer	CT/XR Runoff 2	Success
Filmer	Last page - 4x5	
Filmer	MR 3 stations	Success
Filmer	MR Axial Abdomen	
Filmer	Rectangular 1	Success
Filmer	Rectangular 2	
Filmer	Rectangular 3	
Filmer	Rectangular 4	
Filmer	Spine mixed	
Filmer	Filmer User Prefs	

- In the **User ID** list, select the radio button in front of the user's name you want to import preferences from.

NOTE

Click **Refresh** to update the list of available users.

- In the list that opens, containing all available preferences of the selected user, select or deselect all preferences you wish to import.

The listed preferences are selectable one by one arbitrarily or all together.

NOTE

Before importing the preferences the last column is called **Already exists** and contains **Yes** if the preference already exists.

- Then click the **Import** button to import the preferences from the selected users.

The message "Running" will display during the preferences import and will change to "Success" when done.

The last column, now called **Status**, displays the import status of each selected preferences.

NOTE

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

NOTE

If you are logged as "service", this will import preferences for the user "Service". If you are logged as "Standard", this will import preferences for the user "standard", and so on. So it is important that "clinical" (Standard) users understand how to import other users preferences to their own account. This is explained in the "Importing Preferences manually" Procedure of the **AW Server Administrator Guide** (Online Help), available from the **Service Tools > Documentation** links.

2.5.4.2 Share Preferences

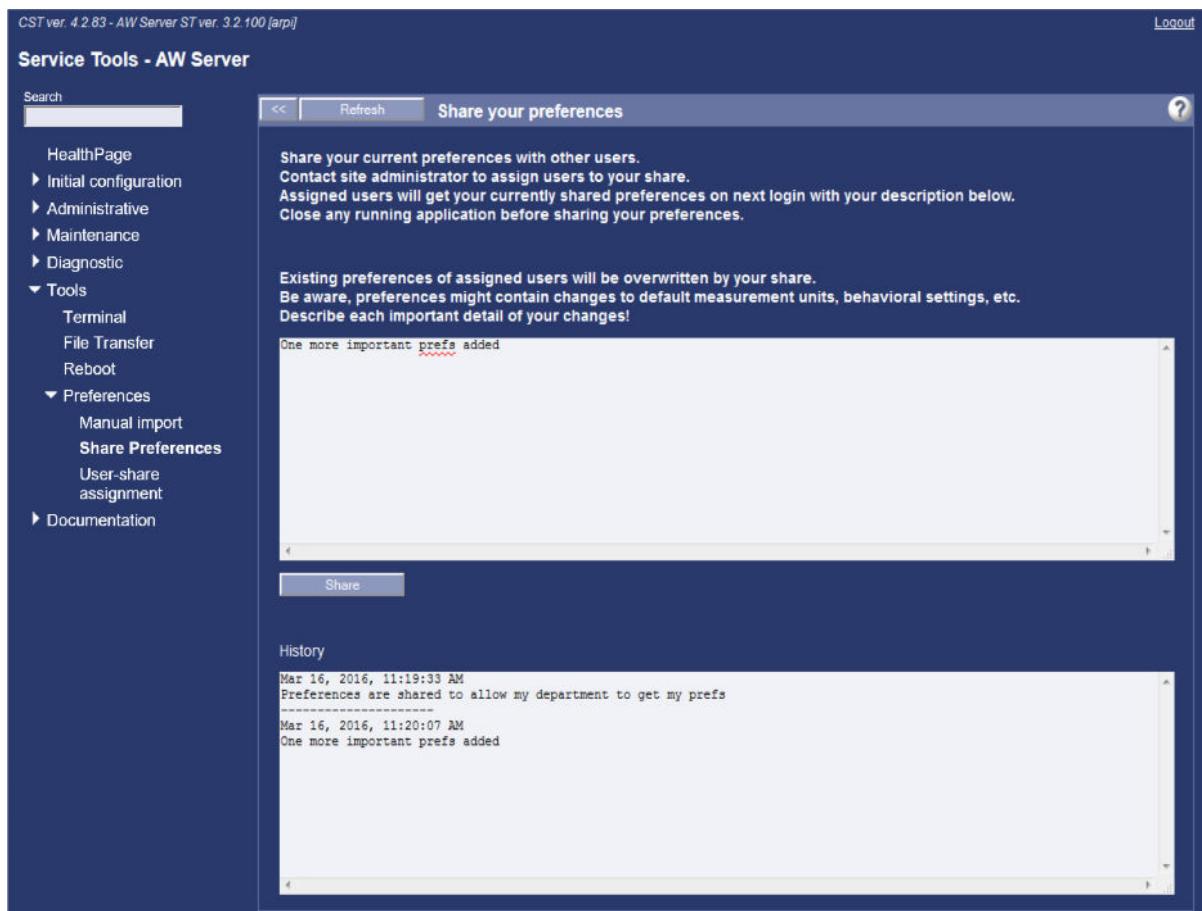
Using this menu, chief radiologists and/or other lead professionals can set up best practice preferences sets and have users assigned to these preferences.

NOTICE

Once a user has shared his/her preferences, the existing preferences of assigned user will be overwritten by this share.

NOTE

User shall close all running applications before sharing his/her preferences.



The procedure for a user to share his/her preferences is presented in details in **AW Server Administrator Guide** (Online Help), available from the **Service Tools > Documentation** links.

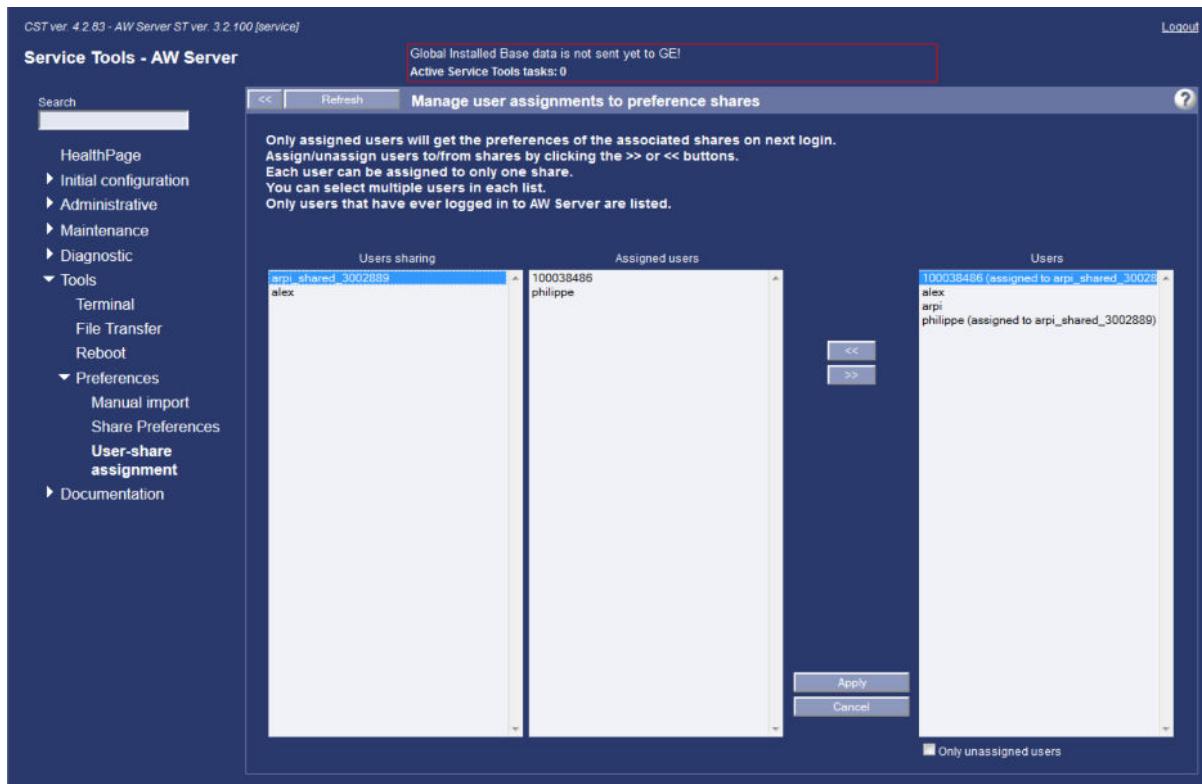
Once the preferences are shared, IT admin can assign them to other users, see menu User-Share assignment below.

2.5.4.3 User-share assignment

Using this menu, the site administrator can assign users to the preferences share that was created by a chief radiologist and/or lead professional.

NOTE

Each user can be assigned to only one share.



Backup/Restore: the user-share assignment configured in this menu are saved as part of the system configuration backup. When restoring the system configuration, the user-share assignments in the backup file are merged with the current user-share assignments. In case of conflict, the user-share assignment in the backup file overwrites the current one.

For more details, refer to the **AW Server Administrator Guide** (Online Help), available from the **Service Tools > Documentation** links.

2.6 HP iLO Service Processor

2.6.1 Overview

AW Server BIOS and Firmware revisions are only a concern to GEHC SERVICE as far as they relate to **HARDWARE** failures. **The first goal in all AW Server service scenarios is to identify whether or not there is a HARDWARE malfunction – period.** For any failure due to HARDWARE, BIOS, or Firmware problems – it is up to HP to resolve...

Even so, it is wise to be aware of the ongoing BIOS and Firmware profile of the product, and have a standard operating procedure to deal with the potential, and to understand what the implications are. **BIOS & FIRMWARE REVISIONS WILL CHANGE REGULARILY IN THE AWS FORWARD PRODUCTION AND IB.**

- The Hardware Vendor (HP) installs most recent BIOS and Firmware updates at installation and documents versions on the "installation hand-off sheet" to the GEHC FE.
- The expectation is that when the server has the most recent BIOS and Firmware update at installation, the server is expected to be completely BIOS / Firmware functional from that point on until when or if something changes - HP issues SCR (supplier change request) or GEHC changes software that effects the BIOS...
- **GEHC is not looking to update the firmware or bios versions, and should not attempt this process.** The hardware vendor does not update BIOS or firmware revisions unless there is a reason to. For the purpose of AW Server support, the reasons to do this will fall into primarily TWO categories:

HP issues an SCR (supplier change request) and implements an update process for the servers in the GEHC IB.

There is a hardware issue identified by GEHC, and dispatched to HP for resolution - which HP determines to require an update to the BIOS and /or firmware.

2.6.2 Checking BIOS and Firmware Revisions

To check the BIOS and Firmware revisions installed on the AW Server:

1. Launch the iLO Web Interface.
 - For iLO 5, see [2.6.3.2 iLO 5 Web Interface on page 102](#).
 - For iLO 4, see [2.6.4.2 iLO 4 Web Interface on page 107](#).
 - For iLO 3, see [2.6.5.2 iLO 3 Web Interface on page 113](#).
 - For iLO 2, see [2.6.6.2 iLO 2 Web Interface on page 118](#).
2. According to the iLO version, select the following:
 - iLO 5: **Firmware & OS Software**
 - iLO 4: **Administration > iLO Firmware**
 - iLO 3: **Administration > iLO Firmware**
 - iLO 2: **Administration > iLO 2 Firmware**.

2.6.3 iLO 5 Service Processor for HPE ProLiant DL360 Gen10 Server

2.6.3.1 iLO 5 Service Processor Setup

iLO 5 is setup during the first installation of Low Tier and High Tier.

After booting up, the iLO 5 configuration menu opens by pressing **<F8>**. The iLO IP address is configured at this step.

Refer to the AW Server 3.2 Hardware Installation Manual for more details on iLO setup.

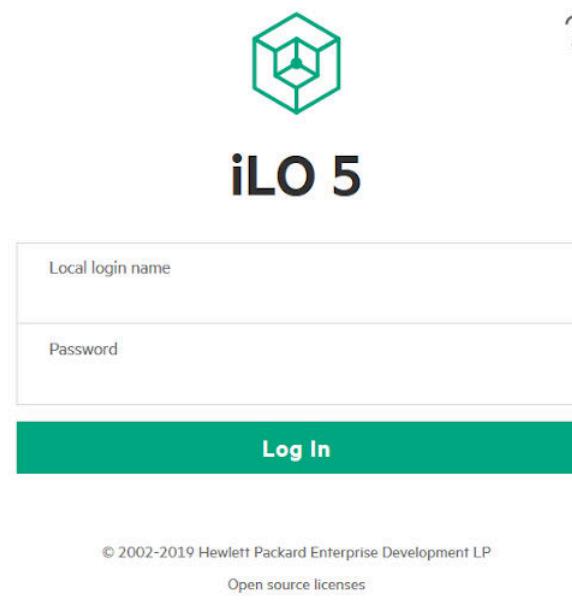
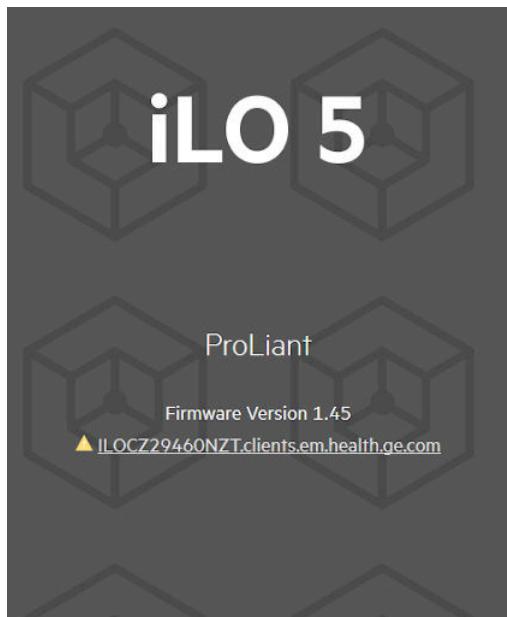
2.6.3.2 iLO 5 Web Interface

This section is a **high-level** overview with related screenshots of the iLO 5 (Integrated Lights-Out 5) Web Interface. It is **not a detailed support tool**.

The iLO 5 provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system.

The iLO 5 Web Interface can be accessed via a web-browser by entering the IP Address of the service processor in the address bar: <http://iLO 5 IP address> (i.e. <http://3.45.24.155>).

The iLO 5 service processor is a separate dedicated component of the server, and has its own unique IP address.



The default login from the vendor is **root** and the default password is **changeme**.

The *Information - iLO Overview* window appears.

- Clicking on **iLO Event Log** displays the event log files.

ID	Severity	Description	Last Update	Count	Category
3386	0	Browser logout: Administrator - 10.107.8.41(DNS name not found).	06/30/2020 08:45:04	1	Security, Administration
3385	0	Browser login: root - 10.107.8.41(DNS name not found).	06/30/2020 08:37:46	1	Security, Administration
3384	0	Browser login: root - 10.107.8.41(DNS name not found).	06/30/2020 08:15:14	1	Security, Administration
3383	0	Browser login: Administrator - 10.107.8.41(DNS name not found).	06/30/2020 08:15:02	1	Security, Administration

- Clicking on **System Information** displays the health of the HPE ProLiant DL360 Gen10 Server hardware.

You can navigate through the different health pages of the server by clicking on the *Processors*, *Memory*, *Network*, *Device Inventory* or *Storage* tabs.

The screenshot shows the 'System Information - Health Summary' page. On the left is a sidebar with links: Information, System Information (which is selected), Firmware & OS Software, iLO Federation, Remote Console & Media, Power & Thermal, Intelligent System Tuning, iLO Dedicated Network Port, iLO Shared Network Port, Remote Support, Administration. The main content area has tabs: Summary (selected), Processors, Memory, Network, Device Inventory, Storage. Below the tabs is a section titled 'Subsystems and Devices' with a table:

↑ Subsystems and Devices	Status
Agentless Management Service	ⓘ Not available
BIOS/Hardware Health	✅ OK
Fan Redundancy	✅ Redundant
Fans	✅ OK
Memory	✅ OK
Network	✅ OK

- Clicking on the *Network* tab displays the MAC address of each Ethernet port.

The screenshot shows the 'System Information - NIC Information' page. On the left is a sidebar with links: Information, System Information (selected), Firmware & OS Software, iLO Federation, Remote Console & Media, Power & Thermal, Intelligent System Tuning, iLO Dedicated Network Port, iLO Shared Network Port, Remote Support, Administration, Security. The main content area has tabs: Summary, Processors, Memory, Network (selected), Device Inventory, Storage. Below the tabs is a section titled 'Physical Network Adapters' with a table for Adapter 1:

Adapter 1 - HP Ethernet 10Gb 2-port 530T Adapter

Location	PCI-E Slot 1
Firmware	7.17.80
Status	✅ OK

Network Ports

↑ Port	MAC Address	IPv4 Address	IPv6 Address	Status	Team/Bridge
1	80:30:e0:20:50:a0	N/A	N/A	✅ OK	N/A
2	80:30:e0:20:50:a4	N/A	N/A	ⓘ Unknown	N/A

- Clicking on **Power & Thermal** > **Server Power** gives access to power on/off of the server.

The screenshot shows the iLO 5 interface with the 'Power & Thermal' tab selected. In the 'Virtual Power Button' section, the 'System Power' status is shown as 'ON'. Below it are four buttons: 'Momentary Press' (Graceful Power Off), 'Press and Hold' (Force Power Off), 'Cold Boot' (Force Power Cycle), and 'Reset' (Force System Reset).

- Clicking on **Momentary Press** shuts down the server.
- Clicking on **Press and Hold** shuts down the server and prevents it from being turned on again locally on the server hardware.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Clicking on the *Temperatures* tab displays the temperatures checked by the sensors. Temperatures are displayed in a Temperature Graph and in a detailed table.

The screenshot shows the iLO 5 interface with the 'Power & Thermal' tab selected. On the left, there is a 'Temperature Graph' showing sensor readings across various components like CPU, Memory, and System. On the right, there is a 'Sensor Data' table listing 20 different sensors with their locations, coordinates, and status.

Sensor	Location	X	Y	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	15	0	OK	30C	Caution: 42C; Critical: 47C
02-CPU1	CPU	11	5	OK	40C	Caution: 70C; Critical: N/A
03-CPU2	CPU	4	5	OK	40C	Caution: 70C; Critical: N/A
04-P1 DIMM 1-6	Memory	8	4	OK	50C	Caution: 90C; Critical: N/A
06-P1 DIMM 7-12	Memory	13	4	OK	47C	Caution: 90C; Critical: N/A
08-P2 DIMM 1-6	Memory	1	4	OK	52C	Caution: 90C; Critical: N/A
10-P2 DIMM 7-12	Memory	6	4	OK	53C	Caution: 90C; Critical: N/A
12-HD Mag	System	11	0	OK	35C	Caution: 60C; Critical: N/A
14-Stor Batt 1	System	5	0	OK	39C	Caution: 60C; Critical: N/A
15-Front Ambient	Ambient	9	1	OK	39C	Caution: 60C; Critical: N/A
16-VR P1	System	11	3	OK	47C	Caution: 115C; Critical: 120C
17-VR P2	System	4	3	OK	51C	Caution: 115C; Critical: 120C
18-VR P1 Mem 1	System	8	2	OK	42C	Caution: 115C; Critical: 120C
19-VR P1 Mem 2	System	13	2	OK	45C	Caution: 115C; Critical: 120C
20-VR P2 Mem 1	System	1	2	OK	46C	Caution: 115C; Critical: 120C

- Clicking on **Remote Console & Media** > **.NET Console** or **HTML5 Console** opens a Terminal window and gives you access to command line login.

.NET Integrated Remote Console (.NET IRC)

The .NET IRC provides remote access to the system KVM and control of Virtual Power and Media from a single console built on the Microsoft .NET Framework.

If you are using Windows 7, 8, 8.1 or 10, a supported version of the .NET Framework is already included in your operating system. The .NET Framework is also available at the [Microsoft Download Center](#). The .NET IRC requires the .NET Framework 4.5.1 or greater.

As a workaround select one of the following instead:

- HTML5 Remote console
- Integrated .NET IRC application with another browser
- Standalone .NET IRC application available from www.hpe.com
- iLO Mobile Application to access the iLO Remote Console

.NET Console

HTML5 Integrated Remote Console

The HTML5 IRC provides remote access to the system KVM and control of Virtual Media from a single console that runs in a supported browser.

HTML5 Console

- Click on **Administration > Licensing**.
- Check that there is a license entered, or enter the license delivered to you into the corresponding fields and click on the **Install** button to save it. If no license is available contact your support center.

License	Status	Activation Key
iLO Advanced	OK	XXXXX-XXXXX-XXXXX-XXXXX-4Q422

Enter License Activation Key

Note: When a new license activation key is installed, the current key is replaced by the new key.

Activation Key

Install

2.6.4 iLO 4 Service Processor for HPE ProLiant ML350p Gen8 Server, HPE ProLiant DL560 Gen8 Server and HPE ProLiant DL360 Gen9 Server

2.6.4.1 iLO 4 Service Processor Setup

iLO 4 is setup during the first installation of Low Tier and High Tier.

After booting up, the iLO 4 configuration menu opens by pressing **<F8>**. The iLO IP address is configured at this step.

Refer to the AW Server 3.2 Hardware Installation Manual for more details on iLO setup.

2.6.4.2 iLO 4 Web Interface

This section is a **high-level** overview with related screenshots of the iLO 4 (Integrated Lights-Out 4) Web Interface. It is **not a detailed support tool**.

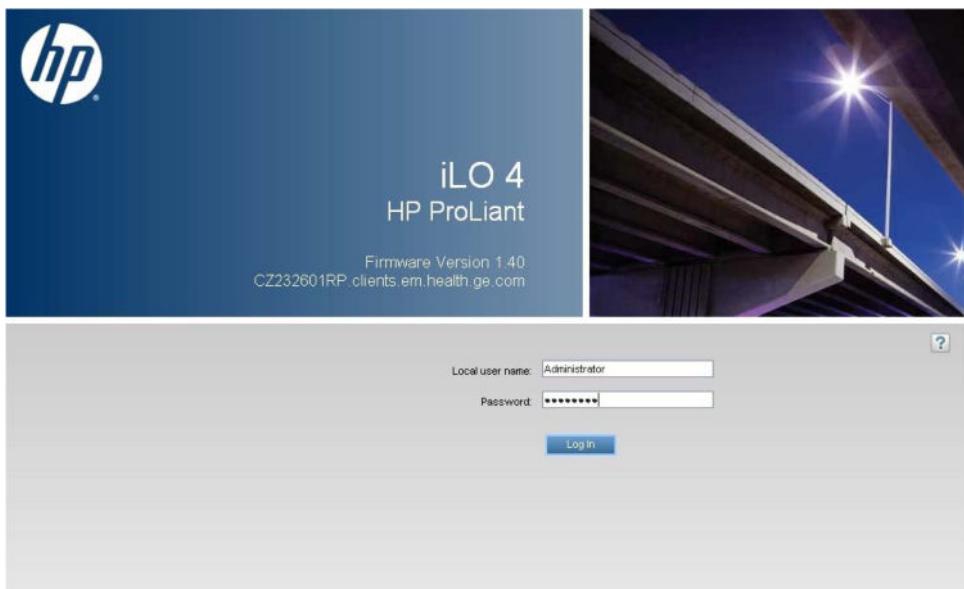
The iLO 4 provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system.

The iLO 4 Web Interface can be accessed via a web-browser by entering the IP Address of the service processor in the address bar: <http://iLO 4 IP address> (i.e. <http://3.45.24.155>).

The iLO 4 service processor is a separate dedicated component of the server, and has its own unique IP address.

NOTE

The iLO 4 Web Interface is slightly different between the HPE ProLiant ML350p Gen8 Server / HPE ProLiant DL560 Gen8 Server (blue color based) and the new HPE ProLiant DL360 Gen9 Server (green color based), but no major change has been brought and the main menus behave the same way. The following example screens have been taken with the HPE ProLiant DL560 Gen8 Server.



The default login from the vendor is **root** and the default password is **changeme**.

The *iLO Overview* window appears.

The screenshot shows the iLO 4 Overview page. On the left, a navigation tree includes 'Information' (selected), 'System Information', 'ILO Event Log', 'Integrated Management Log', 'Active Health System Log', 'Diagnostics', 'Location Discovery Services', 'Insight Agent', 'iLO Federation', 'Remote Console', 'Virtual Media', 'Power Management', 'Network', 'Remote Support', and 'Administration'. The main panel displays 'Information' and 'Status' sections. The 'Information' section lists details like Server Name (aws-DL560), Product Name (ProLiant DL560 Gen8), and various IDs. The 'Status' section shows System Health as 'Degraded' (yellow warning icon), Server Power as 'ON' (green power icon), UID Indicator as 'OFF' (grey circle), TPM Status as 'Not Present', SD-Card Status as 'Not Present', and iLO Date/Time as 'Tue May 13 16:20:57 2014'. Below these are 'Active Sessions' and a table showing a single session for 'Local User: root' at IP 3.249.111.48 via 'Web UI'. At the bottom, status icons show 'POWER: ON' (green), 'UID: OFF' (grey), and a yellow warning icon.

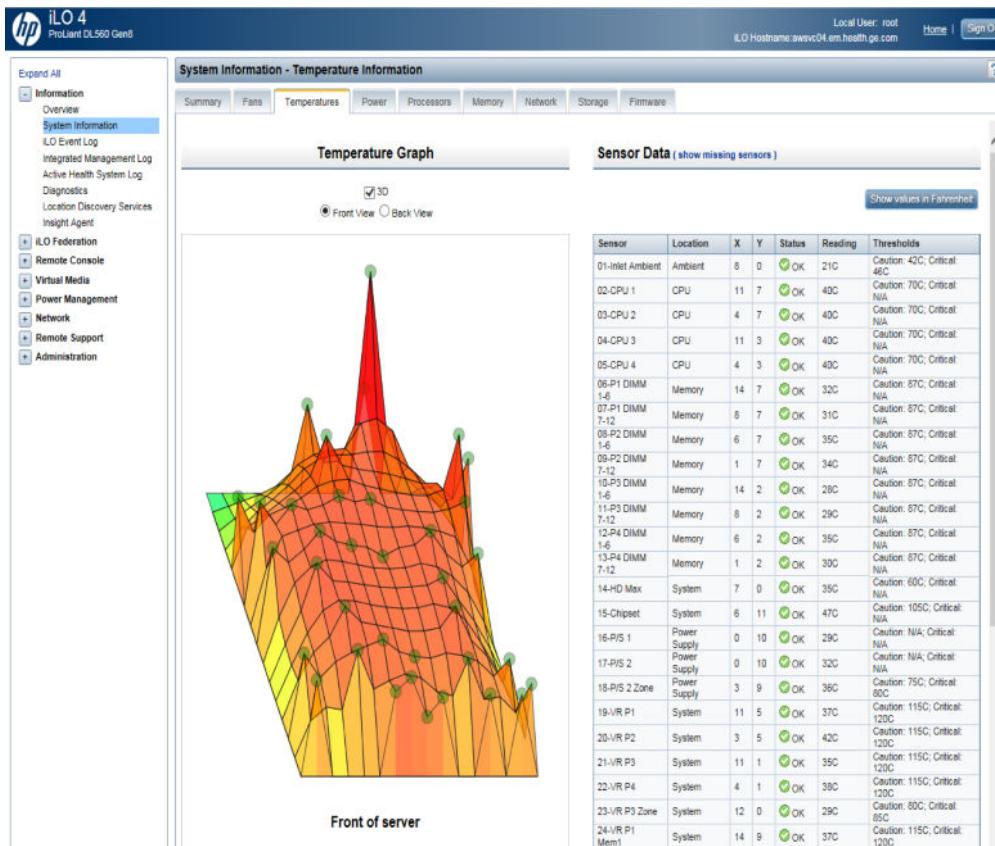
At the bottom of the page, you can click the POWER button to access virtual power buttons of the server.

- Clicking on **System Information** displays the health of the HPE ProLiant DL560 Gen8 Server / HPE ProLiant ML350p Gen8 Server hardware.

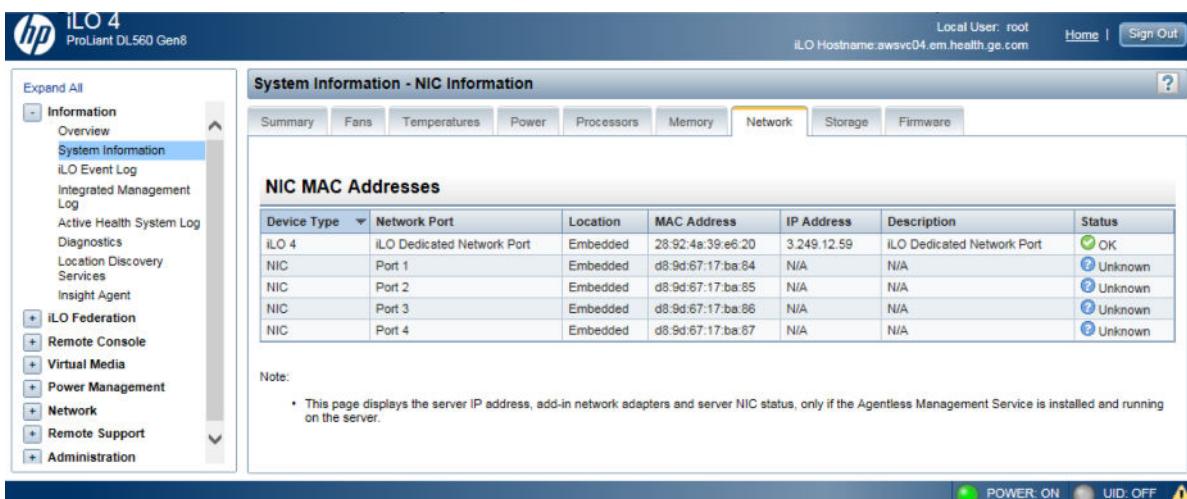
The screenshot shows the 'System Information - Health Summary' page. The navigation tree on the left is identical to the previous screenshot. The main panel has tabs for 'Summary' (selected), 'Fans', 'Temperatures', 'Power', 'Processors', 'Memory', 'Network', 'Storage', and 'Firmware'. The 'Summary' tab shows a table of 'Subsystems and Devices' with columns for 'Subsystems and Devices' and 'Status'. Items listed include BIOS/Hardware Health (OK), Fan Redundancy (Redundant), Fans (OK), Memory (OK), Network (OK), Power Status (Redundant), Power Supplies (OK), Processors (OK), Storage (Degraded), and Temperatures (OK). At the bottom, status icons show 'POWER: ON' (green), 'UID: OFF' (grey), and a yellow warning icon.

You can navigate through the different health pages of the server by clicking on the *Fans*, *Temperatures*, *Power*, *Processors*, *Memory*, *Network*, *Storage* or *Firmware* tabs.

For example, clicking on the *Temperatures* tab displays the temperatures checked by the sensors. Temperatures are displayed in a Temperature Graph and in a detailed table.



Clicking on the Network tab displays the MAC address of each Ethernet port.



- Clicking on **iLO Event Log** displays the event log files.

ID	Severity	Class	Last Update	Initial Update	Count	Description
1505	Informational	iLO 4	05/13/2014 16:16	05/13/2014 16:16	1	Browser login: root - 3.249.111.48(HCE-FF606R1.clients.em.health.ge.com).
1504	Informational	iLO 4	05/13/2014 16:15	05/13/2014 16:15	1	iLO network link up at 1000 Mbps.
1503	Caution	iLO 4	05/13/2014 16:15	05/13/2014 16:15	1	iLO reset by user diagnostics.
1502	Informational	iLO 4	05/13/2014 16:08	05/13/2014 16:08	1	Browser login: root - 3.249.111.48(HCE-FF606R1.clients.em.health.ge.com).
1501	Informational	iLO 4	05/12/2014 18:25	05/12/2014 18:25	1	IPMI/RMCP logout: Administrator - 3.183.16.8 (ukamequals01.em.health.ge.com).
1500	Informational	iLO 4	05/12/2014 18:24	05/12/2014 18:24	1	IPMI/RMCP logout: root - 3.183.16.8(ukamequals01.em.health.ge.com).
1499	Informational	iLO 4	05/12/2014 18:24	05/12/2014 18:24	1	IPMI/RMCP login by Administrator - 3.183.16.8 (ukamequals01.em.health.ge.com).
1498	Informational	iLO 4	05/12/2014 18:24	05/12/2014 18:24	1	IPMI/RMCP login by root - 3.183.16.8(ukamequals01.em.health.ge.com).
1497	Informational	iLO 4	05/12/2014 12:48	05/12/2014 12:48	1	Browser logout: root - 3.249.170.41(hce-cj3blv1-1.clients.em.health.ge.com).
1496	Informational	iLO 4	05/12/2014 11:44	05/12/2014 11:44	1	Remote console session stopped by: root - 3.249.170.41(hce-cj3blv1-1.clients.em.health.ge.com).
1495	Informational	iLO 4	05/12/2014 10:49	05/12/2014 10:49	1	On-board clock set; was 05/12/2014 08:49:55.
1494	Informational	iLO 4	05/12/2014 08:49	05/12/2014 08:49	1	Remote console started by: root - 3.249.170.41(hce-cj3blv1-1.clients.em.health.ge.com).

- Clicking on **Remote Console > Remote Console** opens a Terminal window and gives you access to command line login.

```

iLO 4: htn91 - CZ232601RP.clients.em.health.ge.com
iLO 4
ProLiant DL560 Gen8

Power Switch Virtual Drives Keyboard Help
Local User: Administrator
ILO Hostname:CZ232601RP.clients.em.health.ge.com
Home | Sign Out

Expand All
Information
Overview
System Information
ILO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Location Discovery Services
Insight Agent
ILO Federation
Remote Console
Remote Console
Virtual Media
Power Management
Network
Remote Support
Administration

iLO Integrated Remote Console - Server: htn91 | iLO: CZ232601RP.clients.em.health.ge.com

htn91 login: root
Password:
Last login: Sun Jun 29 13:45:34 from 3.254.101.33
[root@htn91 ~]#

```

NOTE

In the event that you get an error for the status of the .NET Framework NOT, the Microsoft® .NET Framework version is not up to date and needs to be downloaded from the Internet.

- Update first the .NET Framework version to the required 3.5 version.

NOTE

In the event that you would get the following error message and the Terminal window would pop out after a few seconds, it would mean that the license has not been properly entered: An iLO 4 Advanced License is required for continued use after server startup.

- Click on **Administration > Licensing**.
- Check that there is a license entered, or enter the license delivered to you into the corresponding fields and click on the **Install** button to save it. If no license is available, contact your support center.

The screenshot shows the iLO 4 interface under the 'Licensing' section. On the left, a navigation tree includes 'Information', 'ILO Federation', 'Remote Console', 'Virtual Media', 'Power Management', 'Network', 'Remote Support', and 'Administration' (with 'Firmware', 'Licensing', 'User Administration', 'Access Settings', 'Security', 'Management', and 'Key Manager' listed). The 'Licensing' item is selected. The main panel displays 'Current License Status' with a table:

License	Status	Activation Key
iLO 4 Advanced	OK	XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

A note below says: 'You may overwrite the current license key if you have a multi-server activation key, such as one delivered with a flexible-quantity kit or after completing an Activation Key Agreement (AKA).'

The 'Enter License Activation Key' section contains an 'Activation Key' input field with five boxes and an 'Install' button.

- Clicking on **Power Management > Server Power** gives access to power on/off of the server.

The screenshot shows the iLO 4 interface under the 'Server Power' section. The left navigation tree is identical to the previous screenshot. The main panel shows the 'Virtual Power Button' section with 'System Power: ON'. It lists four options: 'Graceful Power Off: Momentary Press', 'Force Power Off: Press and Hold', 'Force System Reset: Reset', and 'Force Power Cycle: Cold Boot'. Below this is the 'System Power Restore Settings' section with the following configuration:

Auto Power-On: Restore Last Power State
 Always Power On
 Always Remain Off

Power-On Delay: Minimum Delay
 15 Second Delay
 30 Second Delay
 45 Second Delay
 60 Second Delay
 Random up to 120 Seconds

A 'Submit' button is at the bottom.

- Clicking on **Momentary Press** shuts down the server.
- Clicking on **Press and Hold** shuts down the server and prevents it from being turned "on" again locally on the server hardware.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Click on **Administration > Firmware** gives access to iLO firmware upgrade utility.

- Click on **Network**.
- Click on **iLO Dedicated Network Port** then click on the *IPv4* tab to access the Network settings.

The Service processor will be restarted in order to take the changes into account, and will not be accessible for login during a few minutes.

2.6.5 iLO 3 Service Processor for HPE ProLiant DL580 G7 Server

This section covers the iLO 3 Service Processor of the HPE ProLiant DL580 G7 Server High Tier.

2.6.5.1 HPE ProLiant DL580 G7 Server Service Processor Setup

The iLO 3 (Integrated Lights-Out 3) service processor configuration can be viewed and set in the HPE ProLiant DL580 G7 Server BIOS setup. Generally speaking, the only real need to ever access the BIOS settings is to either setup and/or view the service processor configuration, or to generally view the current BIOS revision and settings.

NOTICE

Under "normal" operation, there should be no other reason to access the BIOS settings, and IT IS RECOMMENDED NOT TO VENTURE THERE WITHOUT GOOD CAUSE. Server unrecoverable damage could be sustained! Exercise caution...

- The server BIOS can only be accessed by its local KVM or by virtual access to its OS. It cannot be accessed via a remote network command-line connection like telnet or SSH or the like.
- Reboot the server, and press **<F8>** when prompted during the beginning portion of the system start-up to enter the BIOS server set-up utility.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

Refer to the AW Server 3.2 Hardware Installation Manual for more details on iLO setup.

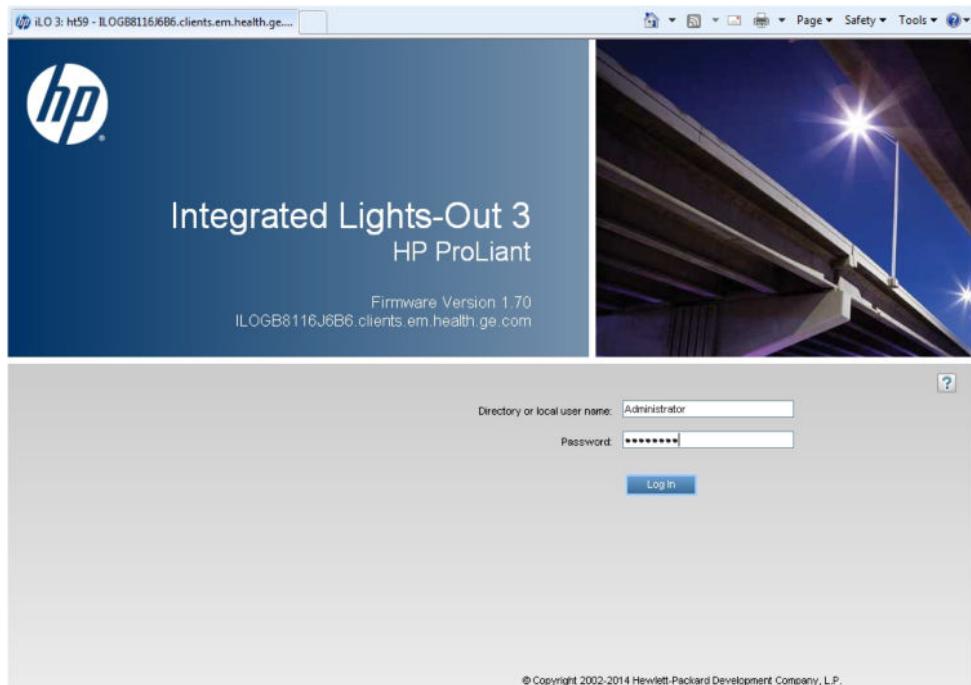
2.6.5.2 iLO 3 Web Interface

This section is a **high-level** overview with related screenshots of the iLO 3 (Integrated Lights-Out 3) Web Interface. It is **not a detailed support tool**.

The iLO 3 provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system.

The iLO 3 Web Interface can be accessed via a web-browser by entering the IP Address of the service processor in the address bar: <http://iLO 3 IP address> (i.e. <http://3.45.24.155>).

The iLO 3 service processor is a separate dedicated component of the server, and has its own unique IP address.



The default login from the vendor is **root** and the default password is **changeme**.

The Information and Status window displays:

Information	
Server Name	aws-06, ProLiant DL580 G7
UUID	38383835-3735-4247-3831-313346424234
Server Serial Number / Product ID	GB8113HBB4 / 588857-B21
System ROM	P65 12/01/2010
Backup System ROM	12/01/2010
Last Used Remote Console	None
License Type	ILO 3 Advanced license is installed.
ILO 3 Firmware Version	1.16 Dec 17 2010
IP Address	3.249.14.171
ILO 3 Hostname	ILOGB8113HBB4.

Active Sessions		
User	IP	Source
Local User: Administrator	3.249.170.62	Web UI

Virtual Buttons

Note: when the UID Indicator is flashing, a critical operation is being performed on the server and should not be interrupted.

Server Power	UID Indicator
Momentary Press	Toggle On/Off
Press and Hold	

- Clicking on **System Information** displays the "health" of the HPE ProLiant DL580 G7 Server hardware.

You can navigate through the different health pages of the server by clicking on the *Fans*, *Temperatures*, *Power*, *Processors* or *Memory* tabs.

For example: clicking on the *Temperatures* tab displays the temperatures checked by the sensors.

For Example, clicking on the *NIC* tab displays the MAC address of each Ethernet port.

- Clicking on **iLO 3 Event Log** displays the event log files.

The screenshot shows the 'iLO 3 Event Log' page. On the left, a navigation menu includes 'Information', 'Overview', 'System Information', 'iLO 3 Event Log' (which is selected and highlighted in blue), 'Integrated Management Log', 'Diagnostics', 'Insight Agent', 'Remote Console' (selected), 'Virtual Media', 'Power Management', and 'Administration'. On the right, a table titled 'iLO 3 Event Log' displays log entries with columns for Severity, Class, Last Update, Initial Update, Count, and Description. The table contains approximately 20 entries, mostly from 'iLO 3' class, with various severity levels (Info, Warning, Error) and descriptions related to server resets and power management.

- Clicking on **Remote Console** opens a Terminal window and gives you access to command line login.

NOTE

In the event that you would NOT get the following status message, the Microsoft® .NET Framework version is not up to date and needs to be downloaded from the Internet.

The screenshot shows the 'Integrated Remote Console' page. The left sidebar has the same navigation menu as the previous screenshot. The main content area shows a message: 'Microsoft .NET Framework 3.5. (available through Windows Update) is required.' Below this, it says 'This machine reports to have the correct version of the .NET Framework 3.5.' At the bottom, there's a 'JVM' tab and a 'Launch' tab, with the 'Launch' tab currently selected. A status bar at the bottom indicates '.NET Version Detected'.

- Update first the .NET Framework version to the required 3.5 version.

NOTE

In the event that you would get the following error message and the Terminal window would pop out after a few seconds, it would mean that the license has not been properly entered.



- Click on **Administration** tab and click to select the **Licensing** sub-menu.
- Check that there is a license entered, or enter the license delivered to you into the corresponding fields and click on the **Install** button to save it. If no license is available, enter the following license or contact your support center.

iLO 3 License for GEHC servers: **332GT-8H665-ZGSWM-BR46M-NJLR2**.

- Clicking on **Power Management > Server Power** gives access to power on/off of the server.

- Clicking on **Momentary Press** shuts down the server.
- Clicking on **Press and Hold** shuts down the server and prevents it from being turned "on" again locally on the server hardware.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Clicking on **Administration > iLO 3 Firmware** gives access to iLO firmware upgrade utility.

http://www.hp.com/go/iLO' and 'This component is also available on the HP ProLiant Firmware Maintenance CD.' At the bottom is a 'Local File' input field with a 'Browse...' button and an 'Upload' button."/>

- Clicking on **Network** allows the Network settings to be changed.

The Service processor will be restarted in order to take the changes into account, and will not be accessible for login during a few minutes.

2.6.6 iLO 2 Service Processor for HP ProLiant ML350 G6 Server

This section covers the iLO 2 Service Processor of the HP ProLiant ML350 G6 Server.

2.6.6.1 HP ProLiant ML350 G6 Server Service Processor Setup

The iLO 2 service processor configuration can be viewed and set in the HP ProLiant ML350 G6 Server BIOS setup. Generally speaking, the only real need to ever access the BIOS settings is to either setup and/or view the service processor configuration, or to generally view the current BIOS revision and settings.

NOTICE

Under "normal" operation, there should be no other reason to access the BIOS settings, and IT IS RECOMMENDED NOT TO VENTURE THERE WITHOUT GOOD CAUSE. Server unrecoverable damage could be sustained! Exercise caution...

- The server BIOS can only be accessed by its local KVM or by virtual access to its OS. It cannot be accessed via a remote network command-line connection like telnet or SSH or the like.
- Reboot the server, and press **<F8>** when prompted during the beginning portion of the system start-up to enter the BIOS server set-up utility.

Refer to the AW Server 3.2 Hardware Installation Manual for more details on the iLO steup.

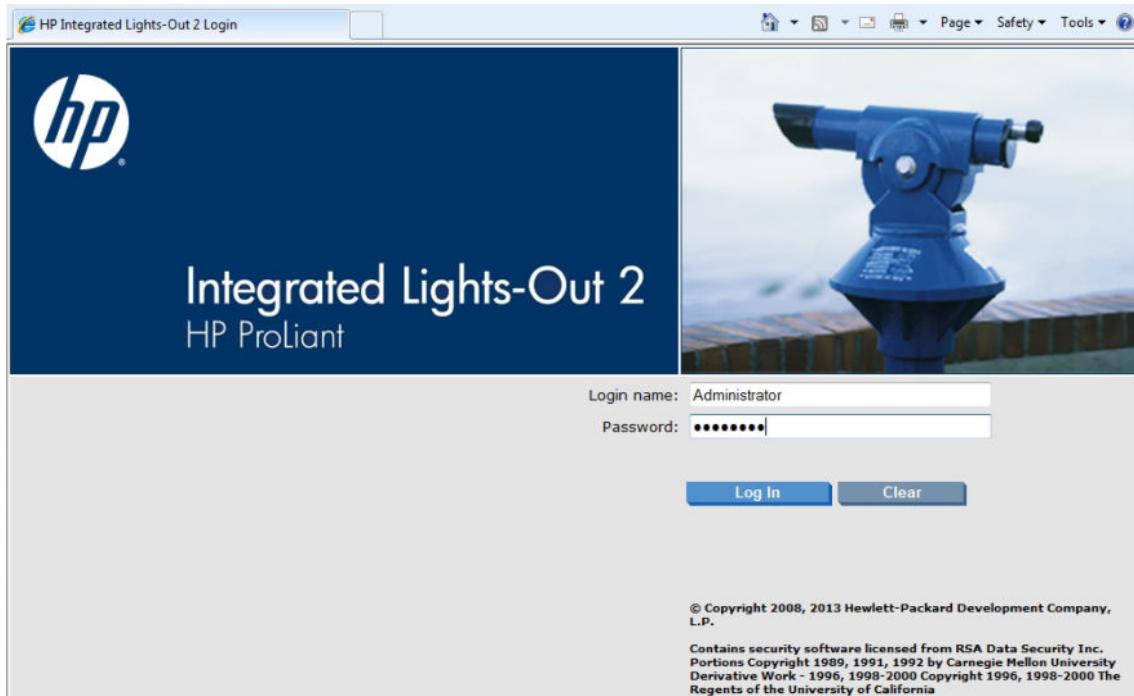
2.6.6.2 iLO 2 Web Interface

This section is a **high-level** overview with related screenshots of the iLO 2 (Integrated Lights-Out 2) Web Interface. It is **not a detailed support tool**.

The iLO 2 provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system.

The iLO 2 Web Interface can be accessed via a web-browser by entering the IP Address of the service processor in the address bar: <http://iLO 2 IP address> (i.e. <http://3.45.12.135>).

The iLO 2 service processor is a separate dedicated component of the server, and has its own unique IP address.



The default login from the vendor is **root** and the default password is **changeme**. However, if the HP ProLiant ML350 G6 Server is delivered with a paper tag hooked to the power supply as shown in illustration below, the default login user is **Administrator** (case sensitive) and the default password is **available on the tag**.

Figure 2-21 Back of the HP ProLiant ML350 G6 Server showing paper tag with iLO 2 password



The **Status Summary** window displays:

Status Summary

Server Name:	host is unnamed ; ProLiant ML350 G6
Serial Number / Product ID:	GB89426CYC / 483448-B21
UUID:	34333834-3834-4247-3839-343236435943
System ROM:	D22 06/01/2009; backup system ROM: 06/01/2009
System Health:	Ok
Internal Health LED:	Ok
Server Power:	Momentary Press <input checked="" type="radio"/> ON Turn UID On <input type="radio"/> OFF Launch Integrated Remote Console
UID Light:	Turn UID On <input type="radio"/> OFF
Last Used Remote Console:	Integrated Remote Console
Latest IML Entry:	(Integrated Management Log is empty)
iLO 2 Name:	IL0GB89426CYC
License Type:	iLO 2 Advanced
iLO 2 Firmware Version:	1.78 06/10/2009
IP address:	3.249.14.162
Active Sessions:	iLO 2 user:Administrator
Latest iLO 2 Event Log Entry:	Browser login: Administrator - 3.249.170.20(DNS name not found).

- Clicking on **Summary** displays the "health" and status page of the HP ProLiant ML350 G6 Server hardware.
- Clicking on **System Information** displays the "health" of the HP ProLiant ML350 G6 Server hardware.

System Health

Summary	Fans	Temperatures	Power	Processors	Memory	NIC
Fans:	Ok; Fully Redundant					
Temperatures:	Ok					
VRMs:	Ok					
Power Supplies:	Ok; Fully Redundant					

You can navigate through the different health pages of the server by clicking on the *Fans*, *Temperatures*, *Power*, *Processors*, *Memory* or *NIC* tabs.

For example, clicking on the *NIC* tab displays the MAC address of each Ethernet port.

The screenshot shows the 'Integrated NIC MAC addresses' page. On the left, a sidebar lists 'System Information' options: Summary, System Log, IML, Diagnostics, iLO 2 User Tips, and Insight Agent. The main content area displays the MAC addresses for Port 1, Port 2, and the iLO 2 itself. A note at the bottom states: 'The MAC addresses of the integrated NICs are shown above. This page does not reflect add-in network adapters.'

	MAC Address
Port 1 NIC MAC address:	00:26:55:86:88:80
Port 2 NIC MAC address:	00:26:55:86:88:81
iLO 2:	00:26:55:86:0D:D4

Clicking on the *Temperatures* tab displays the temperatures checked by the sensors.

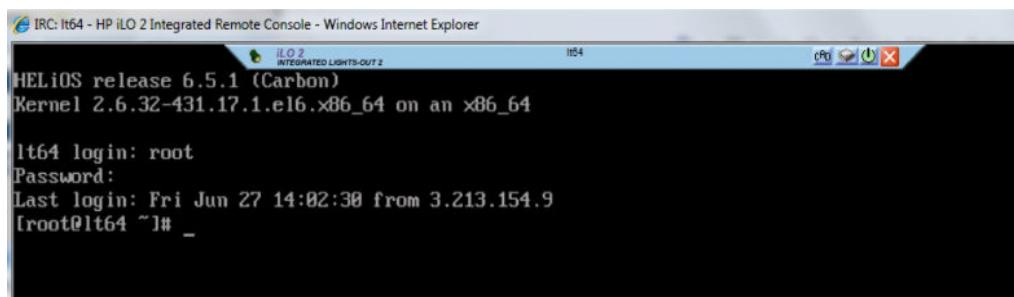
The screenshot shows the 'Temperature Health' page. The 'Temperatures' tab is selected in the navigation bar. The left sidebar shows 'System Information' options. The main content area displays a table of 16 temperature sensors with their locations, statuses, readings, and thresholds.

	<u>Location</u>	<u>Status</u>	<u>Reading</u>	<u>Thresholds</u>
Temp 1:	Ambient Zone	Ok	23C	Caution: 42C; Critical: 46C
Temp 2:	CPU 1	Ok	40C	Caution: 82C; Critical: 83C
Temp 3:	CPU 2	Ok	40C	Caution: 82C; Critical: 83C
Temp 4:	Memory Zone	Ok	40C	Caution: 87C; Critical: 92C
Temp 5:	Memory Zone	Ok	33C	Caution: 87C; Critical: 92C
Temp 6:	Memory Zone	Ok	33C	Caution: 87C; Critical: 92C
Temp 7:	Memory Zone	Ok	32C	Caution: 87C; Critical: 92C
Temp 8:	Memory Zone	Ok	36C	Caution: 87C; Critical: 92C
Temp 9:	Memory Zone	Ok	34C	Caution: 87C; Critical: 92C
Temp 10:	Memory Zone	Ok	38C	Caution: 87C; Critical: 92C
Temp 11:	Memory Zone	Ok	43C	Caution: 87C; Critical: 92C
Temp 12:	I/O Board 7	Ok	42C	Caution: 68C; Critical: 73C
Temp 13:	I/O Board 6	Ok	40C	Caution: 68C; Critical: 73C
Temp 14:	I/O Board 5	Ok	38C	Caution: 68C; Critical: 73C
Temp 15:	I/O Board 4	Ok	36C	Caution: 68C; Critical: 73C
Temp 16:	I/O Board 3	Ok	34C	Caution: 68C; Critical: 73C

- Clicking on **iLO 2 Log** displays the event log files.

Severity	Class	Last Update	Initial Update	Count	Description
Informational	iLO 2	07/23/2009 21:52	07/23/2009 21:52	1	Browser login: Administrator - 3.249.170.20(DNS name not found).
Informational	iLO 2	07/15/2009 22:06	07/15/2009 22:06	1	Browser logout: Administrator - 3.249.170.20(DNS name not found).
Informational	iLO 2	07/15/2009 22:06	07/15/2009 22:06	1	Remote console started by: Administrator - 3.249.170.20(DNS name not found).
Informational	iLO 2	07/15/2009 22:06	07/15/2009 22:06	2	Remote console session stopped by: Administrator - 3.249.170.20(DNS name not found).
Informational	iLO 2	07/15/2009 21:59	07/15/2009 21:59	1	Server power restored.
Informational	iLO 2	07/15/2009 21:59	07/15/2009 21:59	1	Power-On signal sent to host server by: Administrator.
Informational	iLO 2	07/15/2009 21:58	07/15/2009 21:58	1	Server power removed.
Caution	iLO 2	07/15/2009 21:58	07/15/2009 21:58	1	Server reset.

- Clicking on **Remote Console** opens a Terminal window and gives you access to command line login.



- Clicking on **Power Management** gives access to power on/off of the server.

Server Power Controls

Virtual Power Button

Server is currently ON

Momentary Press Press and Hold Cold Boot Reset

Power Configuration Settings

Automatically Power On Server: Yes No

Power On Delay:

Submit

- Clicking on **Momentary Press** shuts down the server.

- Clicking on **Press and Hold** shuts down the server and prevents it from being turned "on" again locally on the server hardware.
- Clicking on **Administration** gives access to iLO firmware upgrade utility.

Upgrade iLO 2 Firmware

Current Firmware: 1.78 06/10/2009

Select New Firmware Image

New firmware image: [Browse...](#)

Send firmware image

iLO 2 firmware update has not started.

Update iLO 2 firmware as follows. For alternatives, consult the help page.

1. Obtain the firmware image (.bin) file from the Online ROM Flash Component for HP Integrated Lights-Out 2. Use the *Extract* option to save the .bin file.

- Clicking on **Network** under **Administration** allows the Network settings to be changed.

Network Settings

Network [DHCP/DNS](#)

NIC: Enabled Disabled Shared Network Port

DHCP: Enabled Disabled

VLAN: Enabled Disabled

VLAN tag:

IP Address: 3.249.14.162

Subnet Mask: 255.255.252.0

Gateway IP Address: 3.249.15.254

ILO 2 Subsystem Name: ILOGB89426CYC

Domain Name:

Link: Automatic 100Mb/FD 100Mb/HD 10Mb/FD 10Mb/HD

Note: The Lights-Out subsystem must be restarted before any changes you make on this screen will take effect.

Apply

Chapter 3 Diagnostics and Troubleshooting

3.1 Overview

This chapter covers the following items:

- Section [3.2 Diagnostic Menu Options](#) on page 124
- Section [3.3 Troubleshooting with FFA](#) on page 144
- Section [3.4 General Troubleshooting](#) on page 153
- Section [3.5 HPE ProLiant DL360 Gen10 Server hardware troubleshooting](#) on page 291
- Section [3.6 HPE ProLiant DL360 Gen9 Server hardware troubleshooting](#) on page 294
- Section [3.7 HPE ProLiant DL560 Gen8 Server hardware troubleshooting](#) on page 302
- Section [3.8 HPE ProLiant DL580 G7 Server hardware troubleshooting](#) on page 308
- Section [3.9 HPE ProLiant ML350p Gen8 Server hardware troubleshooting](#) on page 315
- Section [3.10 HP ProLiant ML350 G6 Server hardware troubleshooting](#) on page 322
- Section [3.11 HP RAID / Disk Subsystem](#) on page 329
- Section [3.12 HPE R/T3000 UPS \(Uninterruptible Power Supply\)](#) on page 342
- Section [3.13 Troubleshooting Virtual AW Server & VMware Platform](#) on page 355
- Section [3.14 Troubleshooting An Integrated Server](#) on page 362
- Section [3.15 Troubleshooting AW Server Clusters](#) on page 363
- Section [3.16 Troubleshooting Client Software](#) on page 367
- Section [3.17 Troubleshooting disk encryption](#) on page 371
- Section [3.18 Log patterns for log analysis in RMF environments](#) on page 379

3.2 Diagnostic Menu Options

The Diagnostics menu of the Service Tools provides the following tool options, which are explained in this section:

- Section [3.2.1 Floating License](#) on page 124
- Section [3.2.2 License Information](#) on page 126
- Section [3.2.3 Log Files Viewer](#) on page 126
- Section [3.2.4 Server and Client Tests](#) on page 138
- Section [3.2.5 Network Test](#) on page 140
- Section [3.2.6 Network Analyzer](#) on page 142

3.2.1 Floating License

To display this option, select **Administrative > Configuration > Floating License** in Service Tools. The *GEMS Floating License Manager* appears. Use this to activate Advanced Applications by entering their floating license keys.

Figure 3-1 Diagnostic - Floating License Manager example

The screenshot shows a software window titled "GEMS Floating License Manager". At the top, it displays "Target Server: Primary (License ID: 00000000, Name/IP: aw-7e15db252ef1 / 3.249.12.232, Version: 'CE')". Below this, it says "License Info (License Key String: CoLA_License_Server, License Key: NNNNNNNNNNNNNNNNNNN)".

Licenses On Media:			Licenses On Server:			
License Key String	License Key	Users	Del	License Key String	License Key	Use
AVA_Xpress			<input type="checkbox"/>	AVA_Xpress	XXXXXXYYYYXXXXXY	6
Advantage_4D_RT_console			<input type="checkbox"/>	Advantage_4D_RT_console	XXXXXXYYYYXXXXXY	6
AngioCARD			<input type="checkbox"/>	AngioCARD	XXXXXXYYYYXXXXXY	6
AngioViz			<input type="checkbox"/>	AngioViz	XXXXXXYYYYXXXXXY	6
AutoBone			<input type="checkbox"/>	AutoBone	XXXXXXYYYYXXXXXY	6
AutoBone_Xpress			<input type="checkbox"/>	AutoBone_Xpress	XXXXXXYYYYXXXXXY	6
CADstream			<input type="checkbox"/>	CADstream	XXXXXXYYYYXXXXXY	6
CARDIQ_FUNC			<input type="checkbox"/>	CARDIQ_FUNC	XXXXXXYYYYXXXXXY	6
CT_Colono_Pro			<input type="checkbox"/>	CT_Colono_Pro	XXXXXXYYYYXXXXXY	6
CT_Perfusion_4D_MultiOrgan			<input type="checkbox"/>	CT_Perfusion_4D_MultiOrgan	XXXXXXYYYYXXXXXY	6
CT_Perfusion_4D_Neuro			<input type="checkbox"/>	CT_Perfusion_4D_Neuro	XXXXXXYYYYXXXXXY	6
CT_Perfusion_4_Neuro_Body			<input type="checkbox"/>	CT_Perfusion_4_Neuro_Body	XXXXXXYYYYXXXXXY	6
CardEP			<input type="checkbox"/>	CardEP	XXXXXXYYYYXXXXXY	6
CardIQ_Function_Xpress			<input type="checkbox"/>	CardIQ_Function_Xpress	XXXXXXYYYYXXXXXY	6
CardIQ_Fusion_PET			<input type="checkbox"/>	CardIQ_Fusion_PET	XXXXXXYYYYXXXXXY	6
CardIQ_Fusion_SPECT			<input type="checkbox"/>	CardIQ_Fusion_SPECT	XXXXXXYYYYXXXXXY	6

NOTE

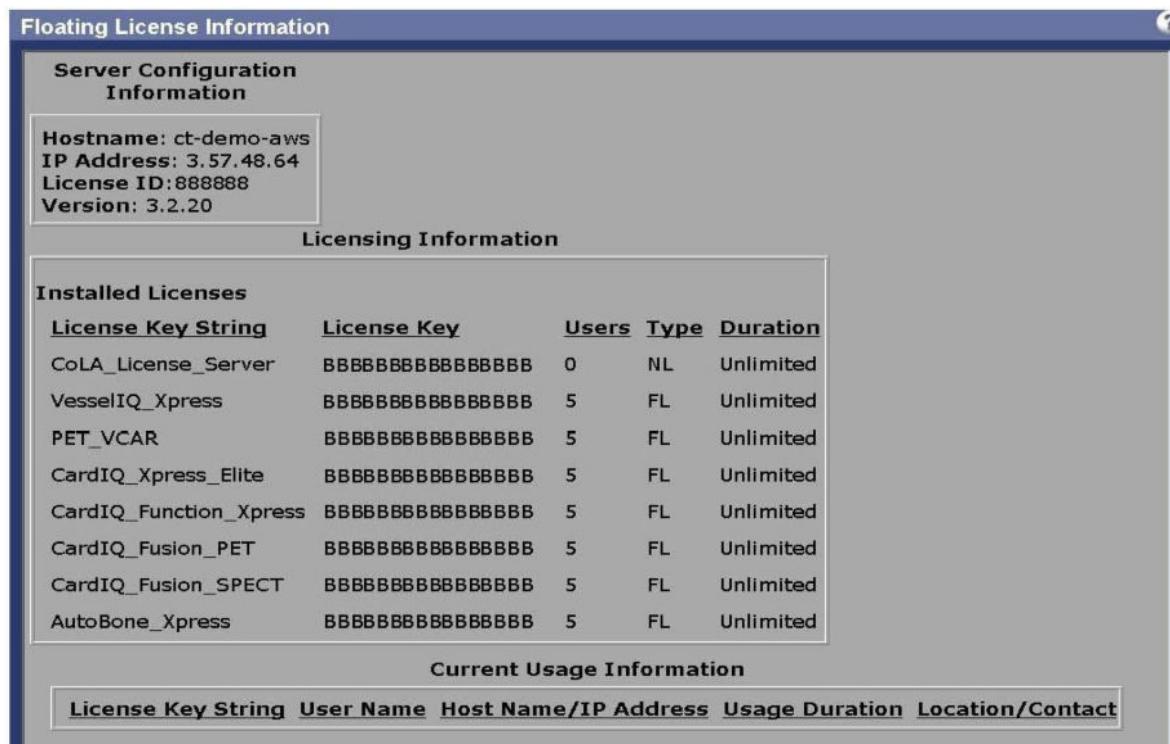
To **manage** Application Licenses installed on the selected Application License Server(s), use the Floating License Manager tool (**Initial Configuration > Licensing > Floating License** in Service Tools). This tool is fully described in the AW Server 3.2 Installation and Service Manual, Floating License configuration menu.

To get a summary of Floating License usage, select **Diagnostic > Floating License** in Service Tools.

This tool is actually a status or information page. It allows to check the overall Floating License configuration and licenses. It also displays the Current Usage Information for these licenses, **which can be a very important tool to help in analyzing licensing issues - if there are no available licenses...**

Think of this as a visual of the license configuration status. The Version number in the header box is the version of the CoLA server on the product.

Figure 3-2 Diagnostic - Floating License Information example



If case of an external Floating License server, refer to the Floating License documentation for more details on configuration and troubleshooting: Floating License 3.3.x Installation Manual 5537368-1EN and Floating License Installation / Service Manual 5149787-100.

3.2.2 License Information

From version AW Server 3.2 Ext. 4.4, from the Service Tools, select **Diagnostic > License Information**.

The page displays the status and usage of the licenses for the components/applications (Web Client and/or the next generation applications) licensed using Flexera licensing (FlexNet Operations (FNO)).

License Information			
Feature Name	Type/Expiry	Total	Used
CardIQ_Suite	permanent	1	0
Webclient	permanent	N/A	0
◀ ▶ 1-2 of 2			

NOTE

Flexera licensing is fully described in the *AW Server 3.2 Installation Manual, Job Card IST008 - Initial Configuration*.

3.2.3 Log Files Viewer

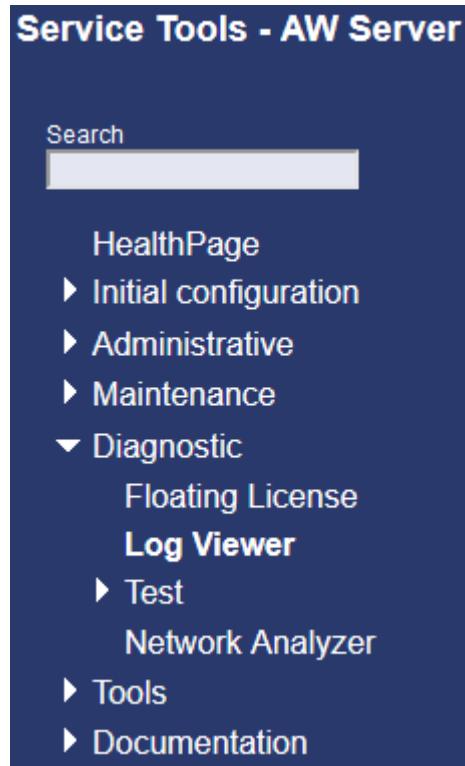
3.2.3.1 Overview

The Log Viewer tool allows the user to remotely view all available system and application log files for the AW Server. It also provides the means to create copies of logs or parts of logs using copy-and-paste.

- From the main menu on the left side of the page, click the **ARROW** next to "Diagnostic" to expand the menu.

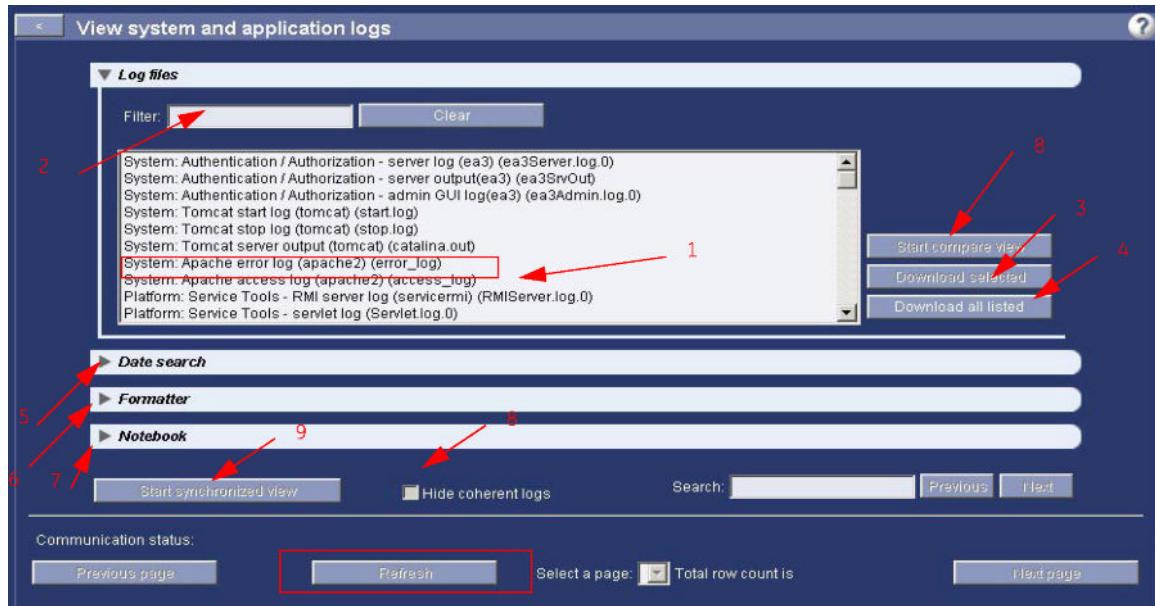
The Log Viewer menu selection will display.

Figure 3-3 LOG VIEWER MENU PATH



- When the Log Viewer menu displays, click the next instance of "**Log Viewer**."

Figure 3-4 LOG VIEWER TOOL

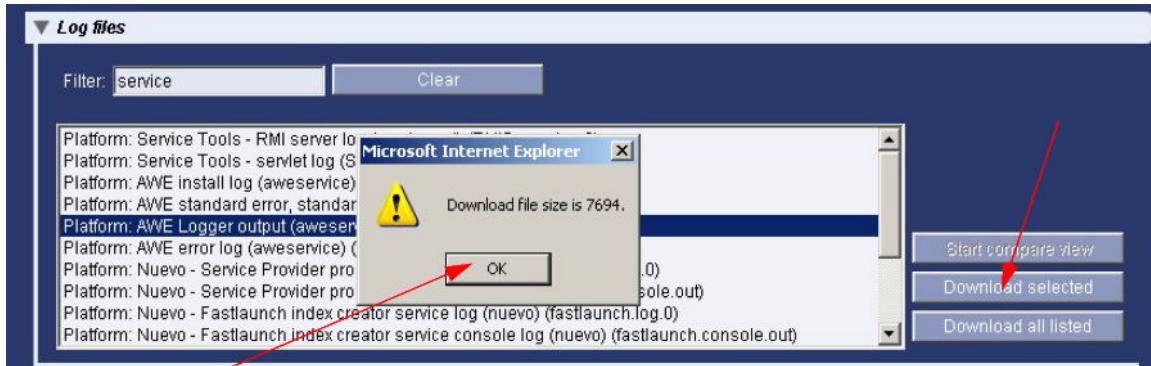


- Log Files list:** This is a list of all the available log files. To select a log scroll up or down through the list, either by clicking the or arrows in the scroll bar, or by placing the cursor over the list and using the mouse scroll wheel to scroll through the contents. When the desired log name appears, click the log name to select it. The contents of the log will display in the **Log file name** area at the bottom two-thirds of the interface.

2. **Filter:** Click in the Filter field and type in the name (or part of the name - i.e: service) of the logfile you want to view, as in the following example:



3. Download selected: This features allows to collect one selected logfile into a compressed file that can be downloaded to the Client PC or FE laptop. The feature gives the size of the compressed logfile collection.



- Click on **OK** to accept.
4. **Download all listed:** This features allows to collect all the listed logfiles into a compressed file that can be downloaded to the Client PC or FE laptop. The feature gives the size of the compressed logfiles collection.

NOTE

If for example, you use no filter, in this case all the logfiles are listed, and the size of the compressed file containing all the logfiles may exceed the 300MB limit allowed. In this case, you will get an error message mentioning that the 300MB limit allowed is exceeded. Use a filter to lower the number of logfiles in the collection, before downloading again.

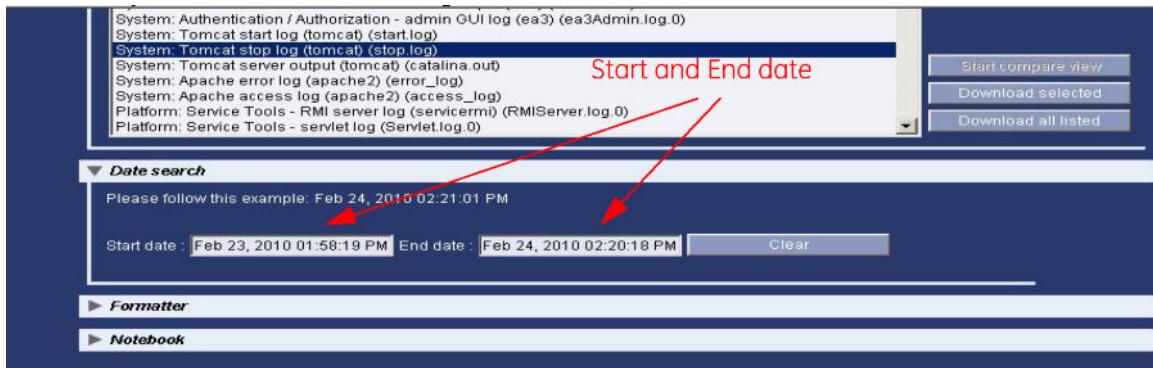
NOTE

Another way to transfer the whole logfiles is to use the File **Transfer tool** (from the Service Tools/ Tools menu). The file Transfer tool compresses the logfiles. Logfiles are located under /export/home/sdc/logfiles directory.

NOTICE

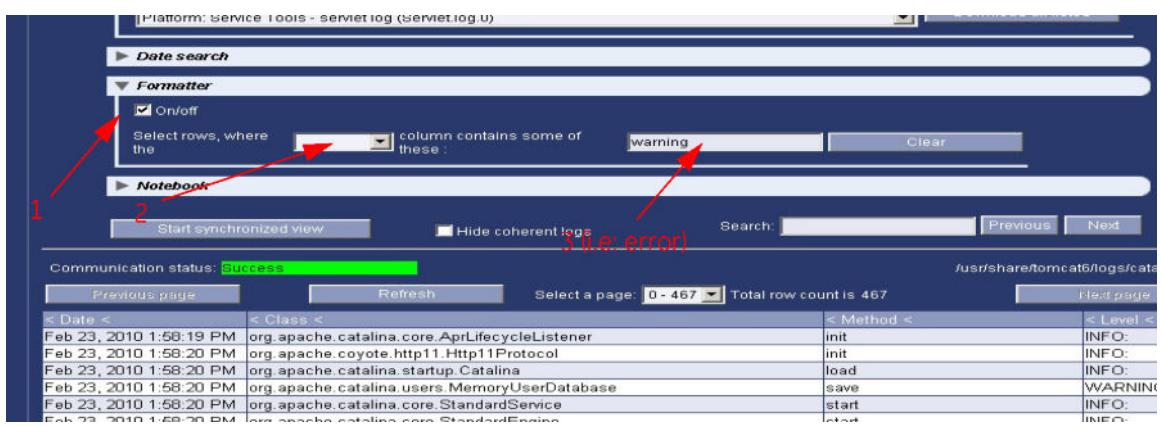
Always use the FFA File Transfer tool to remotely retrieve data from sites for issue analysis.

5. **Date search:** Click on the arrow to expand the menu, then type in the date and time of the event for which you want to review the logs:



- Click on the **Refresh** button.

- 6. Formatter:** Click on the arrow to expand the menu, then click on the on/off button (1), select rows (2), and type in some words that are contained in the event for which you want to review the logs: i.e: "error" (3)

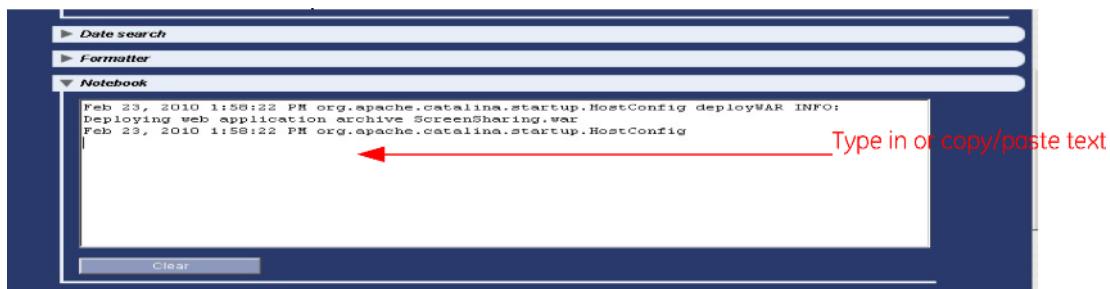


Row selection (2) is either :"Date", "Class", "Method", "Level", "Message"

- Click on the **Refresh** button.

- 7. Notebook:** The Notebook allows you to insert some notes when reviewing the logfiles. This text can be copied into a text file on your PC, that you will be able to send later through email, for example.

- Click on the arrow to expand the menu, then enter text:



- 8. Hide coherent logs:** If similar entries can be found in a row in the log file, then they are hidden (combined to one row) in order to save space during display.
- 9. Start synchronized view:** This is like the result of the command "tail -f FILENAME". It displays the last portion of the file. Automatically updates at every 5 sec.
- 10. Refresh button:** Click this button to **refresh** the logfiles menu and the log contents display. **You can do this to view additional entries that have been made to the log file since you first selected it.** Clicking the Refresh button also selects, by default, the first (lowest) range in the "Log entries" menu, regardless of what range you had selected previously. You can then select the range you need.

11. **Communication status message:** This status message indicates whether or not the most recently selected log file was successfully retrieved.

NOTE

The Communication status message displays for only a few seconds

When a log file is selected for display, the status message, "Reading..." is displayed on a yellow background. This message displays while the Log File Viewer is attempting to retrieve the log file.

If the log file is successfully retrieved, the status message, "Success!" is displayed on a GREEN background.

If the requested log file cannot be found, the message, "The specified log file cannot be found" is displayed on a RED background.

Log file name: This displays the actual file name of the selected log file, along with its path.

Log contents display: Displays the contents of the selected log file up to 1000 lines at a time. You must scroll up and down to view the entire contents of the log file, either by clicking the or arrows in the scroll bar, or by placing the cursor over the list and using the mouse scroll wheel to scroll through the contents.

For logs over 1000 entries: For logs that contain over 1000 log entries, the Log viewer divides the log into two or more smaller sections of up to 1000 entries. You can then select each section via the "Log entries" menu as described previously.

Each page can be selected from the "Select a Page" drop down list.

For example, from the "Log entries" menu shown in the "Pull-Down Log entries Figure," you could select any ONE of the following sections. Each of these sections can be selected via the drop-down "Log entries" menu:

- 1 through 1000,
- 1001 through 2000, and so on, until the final entry,
- 9001 through 9901.

3.2.3.2 Server Log Files

Many gehc software logs are now available from the same location:

/var/log/gehc or /var/log

For example:

/export/home/sdc/logfiles is a symbolic link to /var/log/gehc/sdc/logfiles where platform and application logfiles are captured

/export/home/sdc/nuevo/logfiles is a symbolic link to /var/log/gehc/sdc/nuevo/logfiles

The client-side software logs critical messages to the same log file as the server uses, which is: /
export/home/sdc/logfiles/aweserver.0.0.log

You can tell the difference between client and server log entries based on their content.i.e: client log entries have **user** and the **client host name** included in the message.

- aweservice (a.k.a Solo server) redirects the application logs into nxdisplay_<nxport>.log file instead of merging them into aweservice.log file.
- New logfiles are created for each nx sessions, called hurdle_<nxport>.log. It contains information regarding application lifecycle.
- The logfile directory can be shared through NFS in the AWS cluster, so that service user can collect all logfiles from the cluster on one node easily.
- Solo provides a MEBEF script and registers itself to MEBEF process.

3.2.3.3 Client Log Files

Client logs are also available in separate log files as in example below:

i.e: **/export/home/sdc/client/logfiles/xxxx-xxxx-xxxx-xxxx-global.log** (where xxxx-xxxx-xxxx-xxxx stands for : ClientID_MachineName_TimeStamp_LogType)

3.2.3.4 Copying the Contents of a Log File

Logs can be downloaded from the **Log Viewer** but also from **ftp** tool as shown below

- Click the mouse cursor anywhere on the displayed file, then press "Ctrl" + "A" on the keyboard at the same time to select all the text displayed in the window, even the text which is not visible.
- Then press "Ctrl" + "A" on the keyboard to copy the text. You can then paste it where you need it.

3.2.3.5 Description of Log Viewer Files

NOTE

If the log file is greater than 1000 lines, this will copy only the part of the log that is currently selected in the "Log entries" menu. In other words, you cannot copy more than 1000 lines of any log file at once.

It is more efficient in this case to use the FTP tool in the TOOLS section of the Service Tools – to download the entire log file...

- The following table lists each log file available from the log viewer.
- The table lists the actual file name of each log and a description of what the log contains.
- In the **Log File Name** column – some of the log Files have parenthetical names after them. These names correspond to their software service equivalent listed in the HealthPage – Software Subsystem section.
- **I.E. - If there is a failure in any of the HealthPage Software Subsystem services, you can go directly to the corresponding log(s) - in the Log Viewer tool - for a given service using the parenthetical name.**
- Example > HealthPage Service > **Super Server (aweservice)**
- Log File Name(s) >
- Platform: AWE install log (aweservice)
- Platform: AWE standard error, standard output (aweservice)
- Platform: AWE Logger output (aweservice)
- Platform: AWE error log (aweservice)

3.2.3.6 Logfiles list (non-exhaustive)

NOTE

Some logfiles described below may not be present on the server when the service or the feature is not used. Some logfiles present on the server may not be described below when a new application is installed and has specific logs

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
System: HP hardware log (hp-snmp)	/var/log/hp-snmp-agents/cma.log	All Disk Drive / RAID controller errors and status information details.
System: HP server log	/var/log/hp-health/hpasmd.1og	Hardware errors and status information details.

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
System: received snmp traps	/var/log/snmptraps.log	Contains snmp traps received by the AWS
System: Firewall (pnf)	/var/log/gehc/pnf/logs/managerRunning.log	Firewall rules, e.g., turn on firewall, what filters are applied, etc. The firewall allows only recognized inbound traffic, but outbound traffic is unrestricted.
System: Audit server (eat)	/usr/share/gehc_security/eat/logs/EATLog.0	Audit trail viewer. If there is a problem with the auditing itself, use this log to find the problem.
System: Authentication / Authorization - server log (ea3)	/usr/share/gehc_security/ea3/logs/ea3Server.log.0	Server Authentication/ Authorization problems.
System: Authentication / Authorization - server output (ea3)	/usr/share/gehc_security/ea3/logs/ea3SrvOut	Unknown Authentication/ Authorization problems (i.e., those other than GUI or server log problems).
System: Authentication / Authorization - admin GUI log (ea3)	/usr/share/gehc_security/ea3/logs/ea3Admin.log.0	Authentication/ Authorization problems with the GUI.
System: Tomcat server output (tomcat)	/usr/share/tomcat6/logs/catalina.out	Tomcat runs the Service Tools itself. If Service Tools is failing, check this log. Also check the platform Service Tools servlet log, and the rmi server log.
System: Apache HTTP server error log (apache2)	/var/log/httpd/error_log	Apache Web server error entries
System: Apache HTTP server access log (apache2)	/var/log/httpd/access_log	Access IP entries (i.e., which IP the Apache Web server was accessed from)
System: messages log file	/var/log/messages	Main log file for the operating system. Any OS problem such as an application crash, hardware failure, etc., will show up in this log.
UPS : UPS log	/var/log/gehc/sdc/logfiles/upslog	Captures UPS log
Platform: AWE install log (aweservice)	/usr/tmp/awe_out.log	Captures install log entries (stdout)
Platform: AWE standard error, standard output (aweservice)	/export/home/sdc/logfiles/awerun.log	For debugging purposes only. Overwritten on every server startup, so no history of past messages is maintained.
Platform: AWE Logger output (aweservice)	/export/home/sdc/logfiles/nxdisplay_1000.log	Messages from the aweservice on the server. Clients may also cause important messages to be logged to this file. History is maintained in files with similar names but different numbers, e.g. "nxdisplay_1034.log"
Platform: AWE error log (aweservice)	/usr/tmp/awe_error.log	Captures install errors
Platform: AWS Service Tools - RMI server log (awsservicermi)	/var/lib/ServiceTools_AWS/1og/RMIServer_AWS.log.0	Captures RMI server logs
Platform: AWS Service Tools - servlet log	/var/lib/ServiceTools_AWS/1og/Servlet_AWS.log.0	Captures Servlet logs
Platform: AWE logs	/var/lib/ServiceTools_AWS/1og/WatchDogEnabler.log.0	Captures restart issue failure logs

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
Platform: Service Tools - RMI server log (awsservicermi)	/var/lib/ServiceTools/log/RMIServer.log.0	This log contains information related to Service Tools, for example image deletion.
Platform: Filmer log	/export/home/sdc/logfiles/filmerlog	Filmer application log entries related to user interaction and film generation
Platform: Filmer - Print Job Manager log	/export/home/sdc/logfiles/pjmanagerlog	Captures management of filming queue and history. Lists filmer jobs and pops up when a print error occurs.
Platform: Filmer - Print Builder log	/export/home/sdc/logfiles/printBuilderlog	Contains information about print settings
Platform: Filmer - Print Builder Slave log	/export/home/sdc/logfiles/printBuilderSlavelog	Related to pixel-processing application that creates films to send to the printer
Platform: Print Services - S99 Print Server log (prserver)	/export/home/sdc/logfiles/s99prserver.log	Startup log of the DICOM printer server system service
Platform: Print Services - Print Server log (prserver)	/export/home/sdc/logfiles/prslog	DICOM printer server log. Contains low-level printing management info (filming queue, history, communication with printer...)
Platform: Dicom print log	/export/home/sdc/logfiles/dicomPrintlog	DICOM communication with printer
Platform: Dicom print error log	/export/home/sdc/logfiles/dmsmerge.log	Auxiliary log that captures complementary information on DICOM printing errors.
Platform: RMP Services log (rmpserver)	/export/home/sdc/logfiles/rmpserver.0.0.log, (rmpserver.0.1.log, rmpserver.0.2.log,...)	(Log contains multiple files) RMP Exporter logs. Log messages of the RMPServer Service
Platform: RMP Services output log (rmpserver)	/export/home/sdc/logfiles/rmpserverout.log	The standard output (mainly CSI outputs) of the server. RMPServer Service startup info is logged.
Platform: RMP Audit log (rmpserver)	/export/home/sdc/logfiles/auditlogslog	Audit log info generated by the Filmer and anonymizer applications
Platform: Anonymizer log	/export/home/sdc/logfiles/anonymoussmakerlog	Logs generated when a patient is anonymized.
Platform: Nuevo - Event Router process log (nuevo)	/export/home/sdc/nuevo/logfiles/eventRouter.log.0	Event router server log
Platform: Nuevo - Event Router process console output (nuevo)	/export/home/sdc/nuevo/logfiles/er.console.out	Event router server console log
Platform: Nuevo - Image Importer process log (nuevo)	/export/home/sdc/nuevo/logfiles/imgImporter.log	Dedicated to logging the process to import images into the database.
Platform: Nuevo - Image Importer process console output (nuevo)	/export/home/sdc/nuevo/logfiles/importer.console.out	Image importer console log
Platform: Nuevo - Image Reinstall script log (nuevo)	/export/home/sdc/nuevo/logfiles/restore-images.log	Database restore images log
Platform: Nuevo - Media Manager process log (nuevo)	/export/home/sdc/nuevo/logfiles/mediaManager.log	Reserve space management server log

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
Platform: Nuevo - Media Manager process console output (nuevo)	/export/home/sdc/nuevo/logfiles/mm.console.out	Reserve space management server console log
Platform: Nuevo - Network SCP process log (nuevo)	/export/home/sdc/nuevo/logfiles/nwscp.log	DICOM server log . This file will have all the logging information for store/query/retrieve and storage commit notification providers
Platform: Nuevo - Network SCP process console output (nuevo)	/export/home/sdc/nuevo/logfiles/nwscp.console.out	Console log file for the DICOM Server
Platform: Nuevo - Service Provider process log (nuevo)	/export/home/sdc/nuevo/logfiles/serviceProvider.log.0	Service provider server log. This file has DICOM queue management logs.
Platform: Nuevo - Service Provider process console output (nuevo)	/export/home/sdc/nuevo/logfiles/sp.console.out	Service provider server console log.
Platform: Nuevo - Merge log (nuevo)	/export/home/sdc/nuevo/logfiles/merge.log	DICOM server toolkit log
Platform: Nuevo - nusm script console output (nuevo)	/export/home/sdc/nuevo/logfiles/nusm.console.out	Nuevo system manager console log
Platform: Nuevo - nusm script log (nuevo)	/export/home/sdc/nuevo/logfiles/nusm.log	Nuevo system manager log
Platform: Nuevo - nusm daemon log (nuevo)	/export/home/sdc/nuevo/logfiles/nusmd.log	Nuevo system manager server log
Platform: Nuevo - postgres database server log (nuevo)	/export/home/sdc/nuevo/logfiles/postgreslog	Server log of the postgres patient database
Platform: Nuevo - DB recovery log (nuevo)	/export/home/sdc/nuevo/logfiles/recoverDB.log	Database recovery log
Platform: Nuevo - DB recovery output (nuevo)	/export/home/sdc/nuevo/logfiles/recovery-output.log	Database recovery output
Platform: Nuevo - dbExpressInstall test program log (nuevo)	/export/home/sdc/nuevo/logfiles/terra.log	Database Image install test program log
Platform: Nuevo - UMAI Proxy process log (nuevo)	/export/home/sdc/nuevo/logfiles/umaiproxy.log	UMAI/AIM service provider log
Platform: Nuevo - Dicom server messages trace log (nuevo)	/export/home/sdc/nuevo/logfiles/network_scp_trace.log	DICOM server messages trace log (trace file for DICOM SCP). NOTE: This log will not appear in the log files list unless DICOM trace is enabled for DICOM server.
Platform: Nuevo - Dicom client messages trace log (nuevo)	/export/home/sdc/nuevo/logfiles/network_scu_trace.log	DICOM client messages trace log (trace file for DICOM SCU). NOTE: This log will not appear in the log files list unless DICOM trace is enabled for DICOM client.
Platform: Nuevo - Dicom client messages trace log 2 (nuevo)	/export/home/sdc/nuevo/logfiles/network_scu_trace.log.1	Additional DICOM client messages trace log (trace file for DICOM SCU). NOTE: This log will not appear in the log files list unless DICOM trace is enabled for DICOM client.
Platform: Nuevo - Dicom and Database client log (nuevo)	/export/home/sdc/nuevo/logfiles/nuevo.aweserver.log	LogFile for Nuevo components in the ServerMain JVM. DICOM and database client log . This file contains all the DICOM query and database query initiated from the AW Server browser

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
Platform: Nuevo - Database start-up/shutdown log (nuevo)	/export/home/sdc/nuevo/logfiles/dbxd.log	Log of postgres database start-up/shutdown scripts.
Platform: Nuevo - Fastlaunch index creator service log (nuevo)	/export/home/sdc/nuevo/logfiles/fastlaunch.log.0	Fastlaunch index creator service log (fastlaunch process log). This process is responsible for creating the fast launch index files needed by apps like volume viewer.
Platform: Nuevo - Fastlaunch index creator service console log (nuevo)	/export/home/sdc/nuevo/logfiles/fastlaunch.console.out	Fastlaunch index creator service console log (console output of fastlaunch process)
Platform: Secure Direct connect - system log (secure_dc)	/var/log/messages	Shows Stunnel warning and error messages
Platform: License Server - licensing log (cola)	/usr/share/FL_Server/CoLALicensinglog	Shows licensing request errors for the license server
Platform: License Server - meter log (cola)	/usr/share/FL_Server/CoLAMeterlog	Shows license usage statistics for each user
Platform: License client - licensing log	/usr/share/CoLA/CoLALicensinglog	Shows licensing request errors for the license client
Platform: License client - meter log	/usr/share/CoLA/CoLAMeterlog	Shows statistics for license usage for the license client
Platform: Service Tools - servlet log	/var/lib/ServiceTools/log/servlet.log.0	Any Service Tools feature at any level that fails will trigger an entry in this log. It does not show events outside of Service Tools.
Platform: watchdog log	/var/lib/ServiceTools/log/watchdog/watchdog.log	Captures restart issue failure logs
Application: Install log	/export/home/sdc/logfiles/Install.log	Shows the installation progress for the Volume Viewer (Voxtool) suite of applications. Stores all installation activity details during application install for future debugging and information purposes. Contains plain text data with installation activity information.
Application: PSM log	/export/home/sdc/logfiles/psm.log	Preferences Sharing Manager logs
Application Usage Monitor (Software Metering) log	/var/log/gehc/sdc/logfiles/swmlog	Issues relating to the AUM utility
PACS plug-in	/export/home/sdc/logfiles/PACSplugin.log	Logs relating to library interfacing applications with Dakota plug-in
PACS plug-in	/export/home/sdc/logfiles/pacsintegrun.log	AW integration web service standard output and error
PACS plug-in	/var/log/gehc/sdc/logfiles/pacsIntegWeb.0.0.log	AW integration web service log file
PACS plug-in	/var/log/gehc/sdc/logfiles/dakotaclient.log	Dakota plug-in log file - seamless image decompression and decoding

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
Application: Voxtool log	/export/home/sdc/logfiles/voxtool.log	Log file for execution of Volume Viewer. Contains mainly license checks, selection, user actions, popups displayed, and errors. When voxtool crashes it also generates 2 more files, one with the data set selected voxtool_crash_sel_date.log, and another one appended with the dump of the stack at the time of the crash, voxtool_crash.stack.log.
Cardiq process	/export/home/sdc/logfiles/cardiqprocess.log	LogFile for the CardIQ Xpress Process (CXP) application
Application: CortexID Suite	/export/home/sdc/logfiles/cortexidsuitelog	LogFile for the CortexID Suite application
N/A	/export/home/sdc/logfiles/cortexID_Suite_install.log	Contains a summary of CortexID Suite installation. Details are found in ~sdc/logfiles/Install.log
InSite IIP log	/export/home/sdc/logfiles/	Logs Insite activities and errors
InSite IIP Session log	/export/home/insite/logfiles/iipsession.log	Logs all connectivity activities/status of IIP activities.
RSvP: Axeda gateway log	/opt/InSite/.InSite/Gateway/xGate.log	All activity related to Agent connectivity is captured in the file.
RSvP: Prodiag scheduler log	/opt/InSite/.InSite/Gateway/agentoplogs/prodiagschedule.r.log	Logs related to prodiag job Scheduler are logged.
RSvP: HTTP client log	/opt/InSite/.InSite/Gateway/agentoplogs/httpclient.log	All the activity logs related to sweeps, Prodiags features are captured in the file.
RSvP: Insite log	/opt/InSite/.InSite/Gateway/agentoplogs/insite.log	All the of RSvP Agent feature (Agent registration, AWCCT, Prodiags, sweeps, prodiagScheduler, etc) logs are logged.
RSvP: REST API log	/var/log/gehc/rsrv/rest.log	The log of the RSvP configuration UI on Service Tools.
RSvP: Password Sync log	/var/log/gehc/rsrv/password-sync.log	System user passwords are regenerated in a weekly basis and synchronized to the System Password Vault in GE BackOffice. The log contains the details of this process.
RSvP: iLO update log	/var/log/gehc/rsrv/ilo-update.log	Network settings needed for reaching out iLO of the physical AWServer is sent to the GE BackOffice in a weekly basis. The log contains the details of this process.
Platform: AWS monitor log	/var/log/gehc/awsmonitor.log	AWS system main parameters and daemon processes
Client: Client log messages	/export/home/sdc/logfiles/xdisplay_1000.log	The client-side software logs critical messages to the same log file as the server uses, which is: Platform: AWE Logger output (aweservice)
CSI neta	/export/home/sdc/logfiles/csi_neta.log	Contains bandwidth details for client network communications.

Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
mcelog	/var/log/mcelog	Created by mcelog daemon, in case of performance issues and crash, useful to determine if the problem is Hardware or Software related.
Dotmed logs	/export/home/sdc/logfiles/dotmed_all.log /export/home/sdc/logfiles/dotmed_dataprocessingcpp.log /export/home/sdc/logfiles/dotmed_dataexchangecpp.log /export/home/sdc/logfiles/dotmed_server.log /export/home/sdc/logfiles/dotmed_gsitask.log	The dotmed service (delivered in the .MED rpm) provides an application interoperability platform. It is a platform / CSE component. Captures the standard output and standard error of the .MED server process (Java process that provides the 2 web services: DataProcessing and DataExchange). This also includes the standard output and standard error of any sub-processes launched by the .MED server (such as the process that perform the computations for the DataProcessing service) Log file for the C/C++ DataProcessing client library Log file for the C/C++ DataExchange client library Log file for the .MED server process (it only contains messages logged with the Java java.util.logging API) Log file for the processes that perform the computations for the DataProcessing service
Preprocessing logs	/export/home/sdc/logfiles/preprocessing.log /export/home/sdc/logfiles/preprocessingmgr.log /export/home/sdc/logfiles/preprocServiceWatcher.log /export/home/sdc/logfiles/preloadNotifier.log	This is the logfile for the preprocessing daemon (ie. where series notifications, preprocessing triggering, etc are logged) This is where both standard and error output of preprocessing daemon is dumped. This is the logfile for the preprocessing service (this is the service that starts the daemon) This is the logfile for communications between preprocessing and one process (that especially handles license add/remove management) started by the service.
Autolaunch logs	/export/home/sdc/logfiles/AutoLaunch.log	This is the logfile used by the process that creates preprocessing configuration file used by Service Tools.
Client log	/export/home/sdc/client/logs/fe780042-5ce8-47a2-baa8-fdf70118a53b_HCE-219WN4J_2010.07.20_18.18.04.166_global.log	Example Client global logs

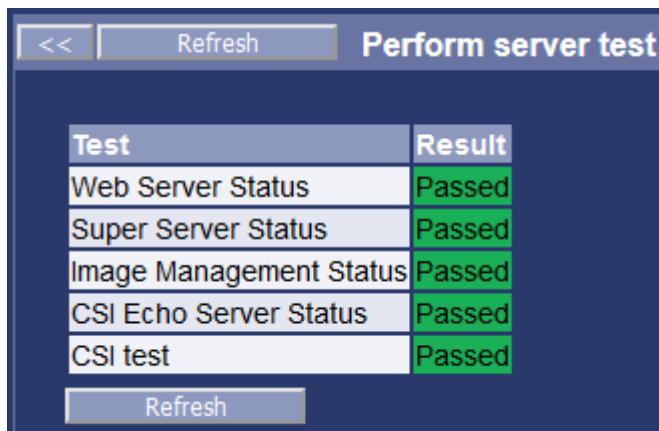
Log file name as displayed by Log Viewer	Actual log file name and path	Description of the log file
Client log	/export/home/sdc/client/log files/fe780042-5ce8-47a2-ba a8-fdf70118a53b_HCE-219WN4J _2010.07.20_16.07.19.995_pe rformance.log	Example Client performance logs
Installation Control Mechanism	/var/log/gehc/sdc/logfiles/icmlog	Contains log for ICM, also called Configuration Registration

3.2.4 Server and Client Tests

The Diagnostics > Test menu in the Service Tools provides tools to poll and test the Server and connected clients.

3.2.4.1 Server Test

This test reports the status of the core services of the server platform., in order to validate whether or not the **server alone** is working correctly or not.



NOTE

In any and all AW Server service scenarios where it is not sure as to where or what the problem is – the server stand-alone test routine in its entirety should be carefully performed to make a service decision as to if the problem is in the server – or in the network/client subsystem. This is extremely important, and is the basis for the service model design of this product. It is equivalent to dividing the “system” in half. And, it is essential to establish the level of responsibility of GEHC service in all service issues.

The **SERVER** is the complete service responsibility of GEHC. This particular test is used as a **PART** of the **STAND-ALONE TEST PROCESS** for the SERVER.

If the server standalone tests have passed, and the configurations in the installation section of this document have been successfully completed - the next step is to verify that a PC client can connect to and use the server.

The easiest way to do this is to identify a client PC on the same local subnet as the server. This will keep potential network issues to a minimum, and make their analysis easier if they exist.

See the AW Server 3.2 Installation and Service Manual, section "Server and Client Installation Validation Tests". You should be able to perform these tests successfully on your target client if the “system” is working correctly. If you can perform the section 3 validation tests on your particular client – or any client, the **AW Server System is fully functional**, and completely validated.

If the **SERVER** stand-alone routine passes, the service responsibility of GEHC switches from a **COMPLETE** ownership model to an **ADVISORY** model. The tools for network and client analysis and

testing should be used to help make suggestions about the potential network or client issue at hand. **The client in particular needs to be tested - with the customer's help - to make sure the "client software" is installed successfully** – but the ultimate ownership of these types of issues is the customer's.

3.2.4.2 AW Server - Client Connectivity Test

After validating the **server standalone** functionality, the next logical, and necessary test is essentially the AW Server “SYSTEM” test. The AW Server does not become the AW Server **system** until a client can connect to it and use it. So, in the technical sense, making sure a client can connect and use the server is actually the FINAL stage of the SERVER standalone rationale.

Because the clients are PC devices that can be anywhere on the network, and can be in various configurations, there is no tool that can be used for GEHC to have complete control of the clients.

This is why the clients are NOT the responsibility of GEHC service

The actual portion of the **CLIENT** that is the responsibility of GEHC is the client application software that gets downloaded and installed on the client. Selection of the client test will perform a set of tests designated to identify possible issues with a client. In reality, there is not much that can be done to remotely analyze and resolve this or other potential client issues, because the client by definition belongs to the user/customer.

- The **CLIENT** tool in the Service Tools **Diagnostic > Test > Client** selection is more of a sensor or status tool that is useful when the client (or clients) are able to connect to the server.
- It is NOT useful at all to diagnose clients that cannot connect to the server.
- Do not confuse this tool with the Client Checker tool, available from the Service Tools login page.
- The **CLIENT** tool can be used for **bandwidth measurement**:
 - in the ServiceTools, go to the **Diagnostic > Test > Client** menu.
 - The list of client currently connected is displayed. If no clients are displayed, use the **Refresh** button. If no clients are connected to the AW Server it is normal that the table is empty.
 - Click on “Click here to measure” on one of the row to begin bandwidth measurement with the corresponding client. A message “Measuring” will display, then the results will display in the cell.
 - Results contain download speed, upload speed, Round Trip Time (RTT) for download and RTT for download. This information can be used to identify issues with the network.

Figure 3-5 Example Diagnostic > test > Client Tool

User ID	Name	Roles	Version	Max. Allocated Memory	Available Memory	# CPUs	Client IP Address	Client Host Name	Bandwidth measurement
john	Dr. John	[STANDARD]	aws-3.1 -0.0- 1426.5	494.9375 MB	17.158203 MB	4	192.168.1.134	HCE-B6HMSY1.clients.em.health.ge.com	↓ 4.93 Mbit/sec / ↑ 2.22 Mbit/sec RTT: ↓ 104.57 ms / ↑ 104.57 ms

Apart from using this tool to analyze connected clients for the above data-points, the following additional factors should be considered when diagnosing **CLIENT** issues – whatever they are:

- Client Login history should be analyzed in the **Diagnostic > Log Viewer** or in **Audit Trail (EAT) > Viewer Tab** tool.
- Was the client ever able to login?

- If so, chances are the client installation was good.
- If not – suspect the client software download installation process or that the client is logged on another server in case of cluster configuration.
- When was the last time of a successful login?
- What was done to or with the client PC since then?
- Perhaps an upgrade?
- Perhaps a re-configuration event?
- Etc...

But, remember that GEHC has the responsibility of the AW SERVER. The responsibility of the **Network** and the associated **Clients primarily belong to the customer**.

NOTE

When there is a cluster of servers, the client is logged on one of the servers, but it may not be obvious which one. The appropriate server can be identified, for example by using the Scalability page of the Service Tools.

NOTE

To test other aspects of Client configuration and specification, use the Client Checker tool available on the Service Tools login page and explained later in this chapter.

3.2.5 Network Test

NETWORK issues are by definition connectivity-related issues, but they can also be performance issues. Depending on your connected location, use basic network tools like “ping” and “traceroute” (see **Ping and Traceroute**) and “wget” ([A.4 WGET on page 470](#)) to verify basic network connectivity. Any client or server that is supposed to be able to use this system should be able to be contacted via **ping** and / or **traceroute – if these services have not been blocked by the site network configuration**.

Likewise, the network bandwidth and download capability should also work using a tool like “wget.”

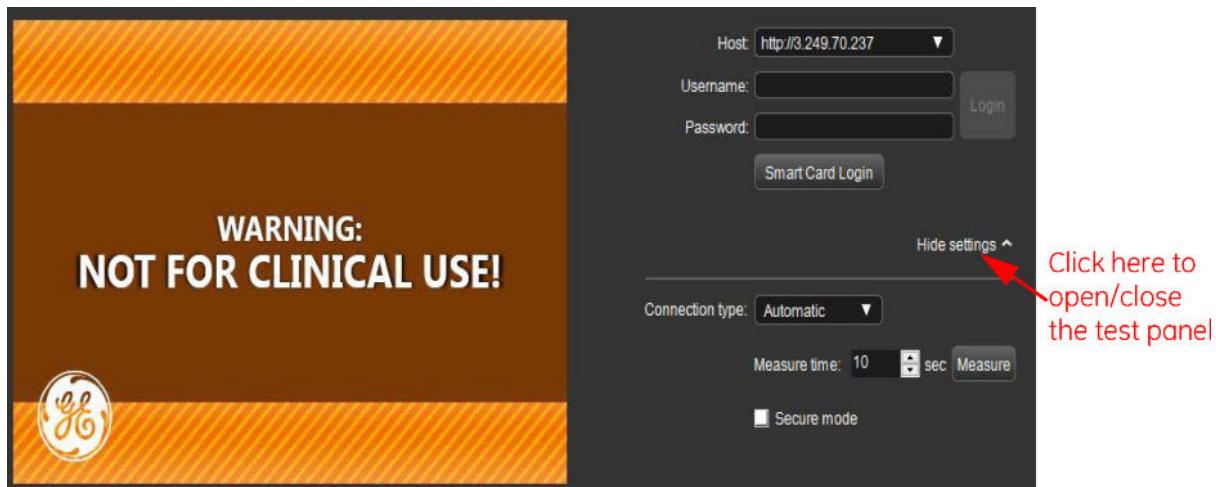
- **PING** – will establish whether there is basic connectivity. (**NOTE:** Some networks block the ping function for security reasons.)
- **TRACEROUTE** – will tell you if network routing is established, and if there might be too many hops involved to support system performance.
- **WGET** – will establish the HTML & FTP connectivity capability, and give you a feel for the bandwidth characteristics of the connection.

If any of these fail, and you have established that the server standalone testing has passed, you are on reasonable ground to suspect a network and / or client related issue.

Do not hesitate to get the site IT admin involved (if they are not already). You (GEHC) may now have limited value-add capability in resolving the problem. Stay engaged, but get the site admin involved based on your results up to this point.

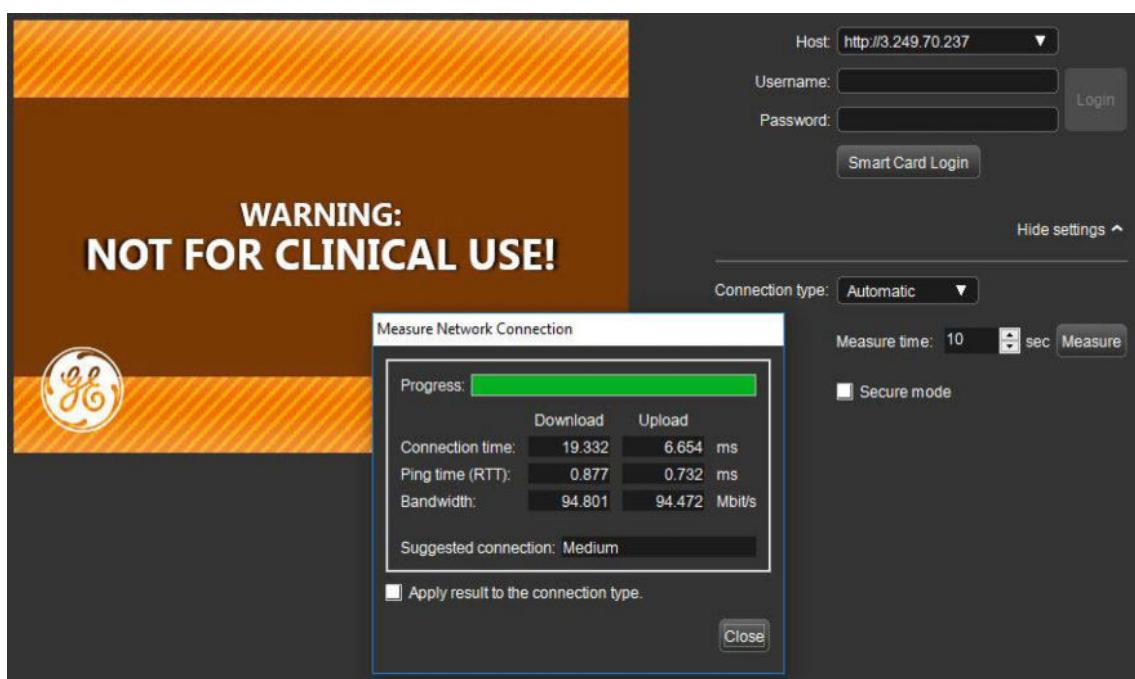
3.2.5.1 Using the Display Performance Measurement Tool (DPMT)

Network / Display performance measurement is also available from the Client login screen as in example below:



- Click on **Show settings** to open / hide the test panel
- Now you can launch the **Measure Network Connection** tool.
- Keep the Connection type: *Automatic*
- Set the measurement time to any suitable value, or keep the default *10 seconds* time.
- Click on the **Measure** button

When the Network Connection measurement has completed, you will get the following result window



As a result of the measurement, the *Suggested Connection* type will be displayed.

- You can click on **Apply results to the connection type** checkbox, then click on the **Close** button to apply the suggested connection type to your Client PC.
- You can check the performance of the network and suggest to your customer, the best compression rate to use, by comparing the results with the table below.

Network speed	Measured network speed	Latency	Compression	non-secure (http)		secure (https)	
				DPMT result	Volume Viewer paging result	DPMT result	Volume Viewer paging result
100 Mbit	94 Mbit	2 ms	1:1	5 fps	4 fps	4 fps	4 fps
			1:15	29 fps	29 fps	27 fps	27 fps
			1:22	30 fps	30 fps	37 fps	28 fps
			1:33	38 fps	30 fps	38 fps	30 fps
500 Mbit	495 Mbit	0 ms	1:1	17 fps	14 fps	12 fps	10 fps
			1:15	42 fps	30 fps	26 fps	28 fps
			1:22	46 fps	30 fps	40 fps	30 fps
			1:33	49 fps	31 fps	47 fps	31 fps
1000 Mbit	884 Mbit	0 ms	1:1	34 fps	26 fps	16 fps	15 fps
			1:15	45 fps	30 fps	42 fps	29 fps
			1:22	46 fps	30 fps	43 fps	30 fps
			1:33	49 fps	31 fps	50 fps	31 fps

- RED: Customer feeling is that performance is bad (below 15 fps)
- GREEN: Customer performance feeling is OK (above 15 fps)
- Measured with ONE user only, and image size on Client PC = 1024 x 1024. Expect performance degradation while resolution increases. Above 2 Mpx, expect exponential degradation.
- Volume Viewer measurements are done on version 10.3 (VS5 version)
- Latency: Expect bad results from 8 ms latency on any network.

In the measurement example above (DPMT), we got a 272.130 Mbit/s bandwidth result for download. This result is between 100 Mbit/s and 500 Mbit/s in the table.

- With 1:1 compression, you can expect a frame rate between 5 fps and 17 fps (in non-secure mode), so performance is not acceptable.
- With 1:15 compression, you can expect a frame rate between 29 fps and 42 fps (non-secure mode), so this compression rate shall be recommended.

3.2.5.2 Server Network Interface Re-configuration

See Chapter 4, Maintenance, [4.7 Network Reconfiguration on page 409](#).

3.2.5.3 Firewall Rules Configuration

See Chapter 4, Maintenance, [4.7 Network Reconfiguration on page 409](#).

For more information about *iptables* and Linux firewalls in general, see www.netfilter.org.

3.2.5.4 Routing Tables Configuration

This is the result example of the **netstat -r** command

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
3.57.48.0	*	255.255.252.0	U	0	0	0 eth0
link-local	*	255.255.0.0	U	0	0	0 eth0
loopback	*	255.0.0.0	U	0	0	0 lo
default	medmfp2us.med.q	0.0.0.0	UG	0	0	0 eth0

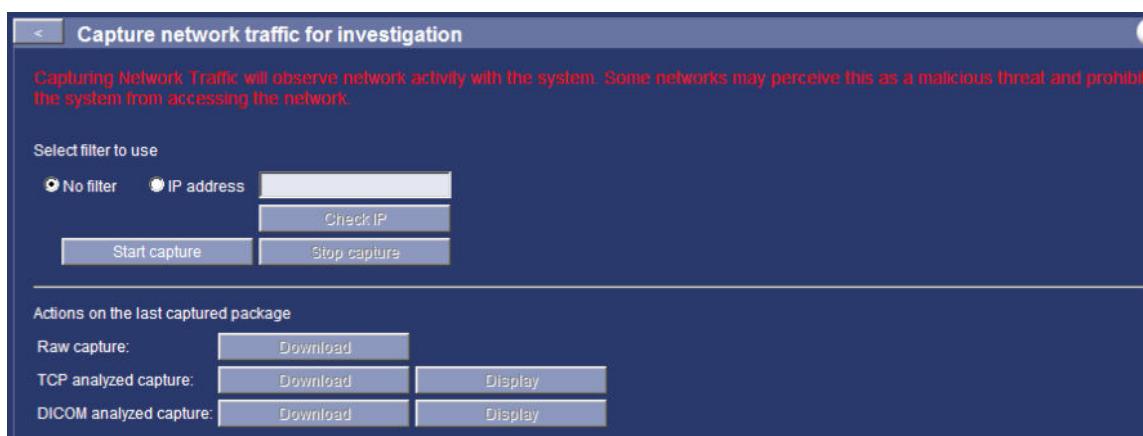
3.2.6 Network Analyzer

3.2.6.1 Function

This Service Tool is a basic network packet capture tool – similar to tools like "Ethereal, Wireshark, or tcpdump." It captures the data on the server's public or applications port or network interface at the packet level.

The tool allows filtering, to the extent that you can choose to either capture **ALL packet traffic**. (No filter) or just the traffic to a **particular IP Address** – which needs to be entered - if this option is selected. There is also a Check IP button to test the basic connectivity of the IP Address entered.

Figure 3-6 Diagnostic > Test > Network Analyzer



Here is the network capture workflow:

- Select either no filter or enter the IP Address of the particular network target you want to analyze.
- Begin the network activity that you want to examine the packets from.
- Click the **START capture** button. After a few moments, a yellow status message **Capturing...** displays.
- After sufficient time, click the **STOP capture** button. A green status message **Success** should display.
- **Recommendation** – capture data for only as long as is necessary to sample the activity in question. The less data you have to analyze, the better. Depending on network traffic, the capture data set can become very – very large.
 - The data package processing buttons in the lower part of the screen are now active. Select whether to download or display the raw, TCP analyzed or DICOM analyzed data, if available. (If there is no TCP or DICOM data, an appropriate message will display.)
 - If you select **Download**, a popup will appear indicating the size of the download (capture) file.
- Click **OK**, and another popup will display showing the **Name, Type, and IP Address Source** of the file, and asking you if you want to **Open** or **Save** the zip file.

NOTICE

The Open option requires an application capable of opening zip files.

- The Save button lets you save the zip file must be saved on your host PC, or the back-office of the FFA File Transfer tool, and then pulled to a PC that can install and run one of the network packet analysis tools like *Ethereal*, *Wireshark*, or *tcpdump*.

- After saving the capture file, you must extract it from its “zipped” format. You can open the resultant file (example file name format AWS_network-capture_20080725-154156) and analyze the data ONLY by opening it with a capture tool like *Ethereal*, *Wireshark*, or *tcpdump*.

NOTICE

Use this tool advisedly.

BE ADVISED THAT CAPTURING NETWORK TRAFFIC AT THE PACKET LEVEL IS AN INTRUSIVE NETWORK ACTION. CAPTURING NETWORK TRAFFIC WILL OBSERVE NETWORK ACTIVITY WITH THE SERVER.

SOME NETWORKS MAY PERCEIVE THIS AS A MALICIOUS THREAT AND PROHIBIT THE SERVER FROM ACCESSING THE NETWORK.

ALWAYS CONSULT WITH IT ADMIN BEFORE USING THIS TOOL...

3.2.6.2 Testing the Client (Windows®) Operating System

It is not necessary to test the **WINDOWS OS** client operating system separately. If the client PC passes the network test and the client checker test, then the operating system is performing correctly.

3.2.6.3 Testing the Client (Linux) Operating System

Linux OS are currently not supported for the Client at the current time of release. Certain GE consoles might support Linux Client. See the corresponding console User Guides for further details

3.3 Troubleshooting with FFA

3.3.1 Retrieving Passwords from FFA

The FFA users can retrieve the passwords from the GE Backoffice for the systems remotely connected with Insite or RSvP.

3.3.1.1 Retrieving the passwords in Insite

The system passwords can be retrieved from the GE Backoffice.

1. Remotely through FFA, display the **Re-Checkout** panel.

Connection Information (NETWORK)	
IP Connection Information	
Local IP Address	3.249.70.226
Network Address Translation IP	10.99.93.48
SPA Id	null
Comments	SYSTEM'S ETHERNET PORT
Passwords	
Login ID	Password
sdc	odw2.0
root	Tod&bu
insite	Geiaw@08

2. In the **Checkout** tab view the passwords.

3.3.1.2 Retrieving the passwords in RSvP

The passwords for root and *filetransfer* system users/accounts and the password for *service* can be retrieved from the GE Backoffice.

1. Remotely through FFA, display the **System Password Vault** panel.

Showing 3 configured accounts for System ID **AWBUCLAB162**

#	App Name	Username	Password	Last Updated	Updated By	Actions
1	ea3	service	*****	Jun-03-2021 10:41:26	AGENT	Show Copy Change Password
2	sftp	filetransfer	*****	Jun-14-2021 19:07:31	AGENT	Show Copy Change Password
3	ssh	root	*****	Jun-14-2021 19:07:34	AGENT	Show Copy Change Password

2. Select the **Show** link to view the passwords.

3.3.2 Accessing Service Tools from FFA

If using a remote connection (Insite/RSvP), the Service Tools can be accessed remotely through FFA.

1. Remotely through FFA, start the Service Tools using the FFA connectivity tool.

- For Insite connectivity (version prior to AW Server 3.2 Ext. 4.2), launch the **CSD Redirect** connectivity tool:



NOTE

Connectivity tools require the use of the FTA client to make the connection work. FFA displays a warning if it needs to be installed. Refer to the *FFA documentation* for more details on FFA usage.

A pop-up appears mentioning that CSD Redirect has limited functionality in the Google Chrome browser. Click on **Continue** to acknowledge the pop-up.

- For RSvP connectivity (from version AW Server 3.2 Ext. 4.2):

- Launch the **HTTPS** connectivity tool:

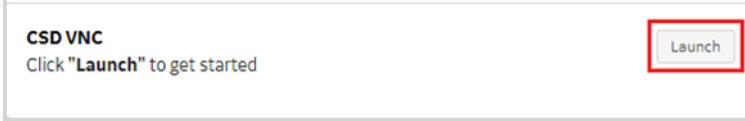


NOTE

Connectivity tools require the use of the ACA helper software and the FTA client to make the connection work. FFA displays a warning if it needs to be installed. Refer to the *FFA documentation* for more details on FFA usage.

OR

- Launch the **CSD VNC** service tool:



2. If using **HTTPS** connectivity tools, when the window loads, copy the URL from the Chrome address bar and paste it into a new Internet Explorer (or in a Chrome IE tab) or Firefox session.

3. If pop-ups related to the security certificate appear, acknowledge them.

The login page appears.

4. Log into the Service Tools and navigate through the Healthpage and through the different menus as described in [2.2 Service Tools Overview on page 51](#).

3.3.3 Accessing iLO from FFA

3.3.3.1 iLO cannot be directly accessed from FFA

In case of Insite connectivity or if the iLO cannot be directly accessed from FFA for any means, it is possible to access the command line interface of the iLO using FFA.

1. Connect to FFA.
2. In FFA, use the **SSH** connectivity tool or the **Terminal** tool in FFA to connect to the AW Server.
3. From the command line, start an ssh connection to the iLO:

```
ssh XX.XX.XXX.XXX -l root <Enter> (where XX.XX.XXX.XXX is the IP Address of the iLO)
```

4. When asked, enter the **root** password for iLO (default value: **changeme**).

You are now connected to the iLO.

5. Use the command **help** to display the list of available commands, as shown below:

```
</>hpiLO-> help

status=0
status_tag=COMMAND COMPLETED
Thu Sep 4 15:29:32 2014
DMTF SMASH CLP Commands:
help : Used to get context sensitive help.
show : Used to display values of a property or contents of a collection
target.
show -a : Recursively show all targets within the current target.
show -l <level> : Recursively show targets within the current target
based on 'level' specified.
Valid values for 'level' is from 1 to 9.
create : Used to create new instances in the name space of the MAP.
Example: create /map1/accounts1 username=<lname1> password=<pwd12345>
name=<dname1> group=<admin,config,oemhp_vm,oemhp_rc,oemhp_power>
delete : Used to destroy instances in the name space of the MAP.
Example: delete /map1/accounts1/<lname1>
load : Used to move a binary image from an URL to the MAP.
Example : load /map1/firmware1 -source http://192.168.1.1/images/fw/
iLO4_100.bin
reset : Causes a target to cycle from enabled to disabled and back to
enabled.
set : Used to set a property or set of properties to a specific value.
start : Used to cause a target to change state to a higher run level.
stop : Used to cause a target to change state to a lower run level.
cd : Used to set the current default target.
Example: cd targetname
date : Used to get the current date.
time : Used to get the current time.
exit : Used to terminate the CLP session.
version : Used to query the version of the CLP implementation or other
CLP elements.
HP CLI Commands:
POWER : Control server power.
UID : Control Unit-ID light.
NMI : Generate an NMI.
VM : Virtual media commands.
LANGUAGE : Command to set or get default language
```

VSP : Invoke virtual serial port.
TEXTCONS : Invoke Remote Text Console.

NOTE

Command line can be used to manage power of the AW Server as well as UID. Command lines provide access to the sensors values, however the results do not display in a way that is easy to interpret. For access to sensor values, use the **ipmitool** and **hpncfg** commands (from the AW Server command line).

The following commands are especially useful:

Command	Effect
power	Displays the current server power state
power on	Turns the server on
power off	Turns the server off
power off hard	Force the server off using press and hold
power reset	Reset the server
UID off	Turns the UID LED off
UID on	Turns the UID LED on

6. To leave the iLO Command line, use the command **exit**:

exit <Enter>

3.3.3.2 iLO can be directly accessed from FFA

In case of RSvP connectivity (from version AW Server 3.2 Ext. 4.2), the iLO can be directly accessed from FFA.

1. Remotely through FFA, start the iLO Web Interface using the FFA iLOM Connectivity:



The iLO Web Interface login page opens in a separate tab.

NOTE

In some cases the iLO Web Interface does not launch with error "Failed to obtain device credentials". If the issue occurs, wait a few minutes and try again

2. Log into iLO Web Interface as described in [2.6 HP iLO Service Processor on page 101](#).

3.3.4 Troubleshooting with Screen Sharing

3.3.4.1 Screen Sharing feature

The Screen Sharing feature purpose is to allow the Service Engineer to remotely manage the User's desktop, in order to better understand the AWS User's issues.

This can be done remotely through FFA, using the Service Tools.

NOTE

Screen Sharing feature is note applicable in Secured for RMF mode.

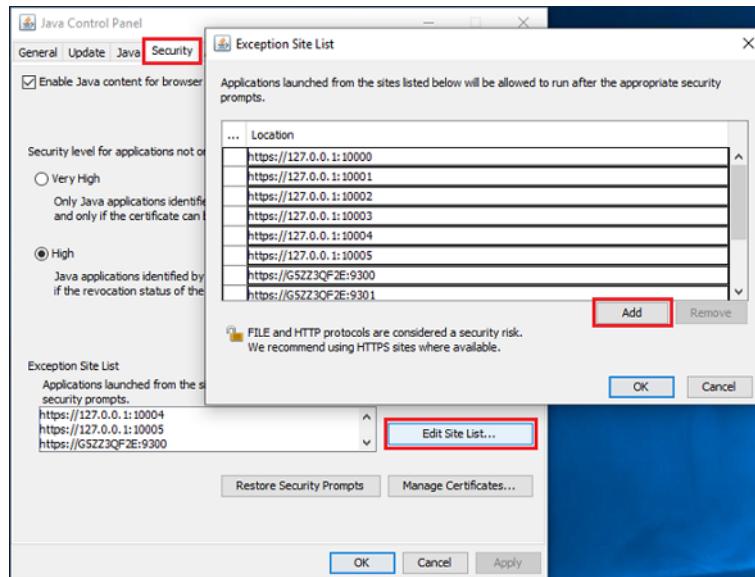
NOTE

Screen Sharing menu cannot be accessed with Chrome 43 and 45, and Firefox from version 53. Use Firefox (version prior to 53) or Internet Explorer browser instead.

NOTE

When using IE11, apply the following setup:

1. To prevent the security settings from blocking Java, add server https URL to the Exception Site List:
 - a. In **Control Panel > Java > Security**, select **Edit Site List**.



- b. Click on **Add** to enter the IP address of the AW Server:
 - For InSite connectivity (version prior to AW Server 3.2 Ext. 4.2):

https://hostname:port#

To get the **hostname**, type **hostname** in a command prompt.
port# is from **9300**.
 - For RSvP connectivity (from version AW Server 3.2 Ext. 4.2):

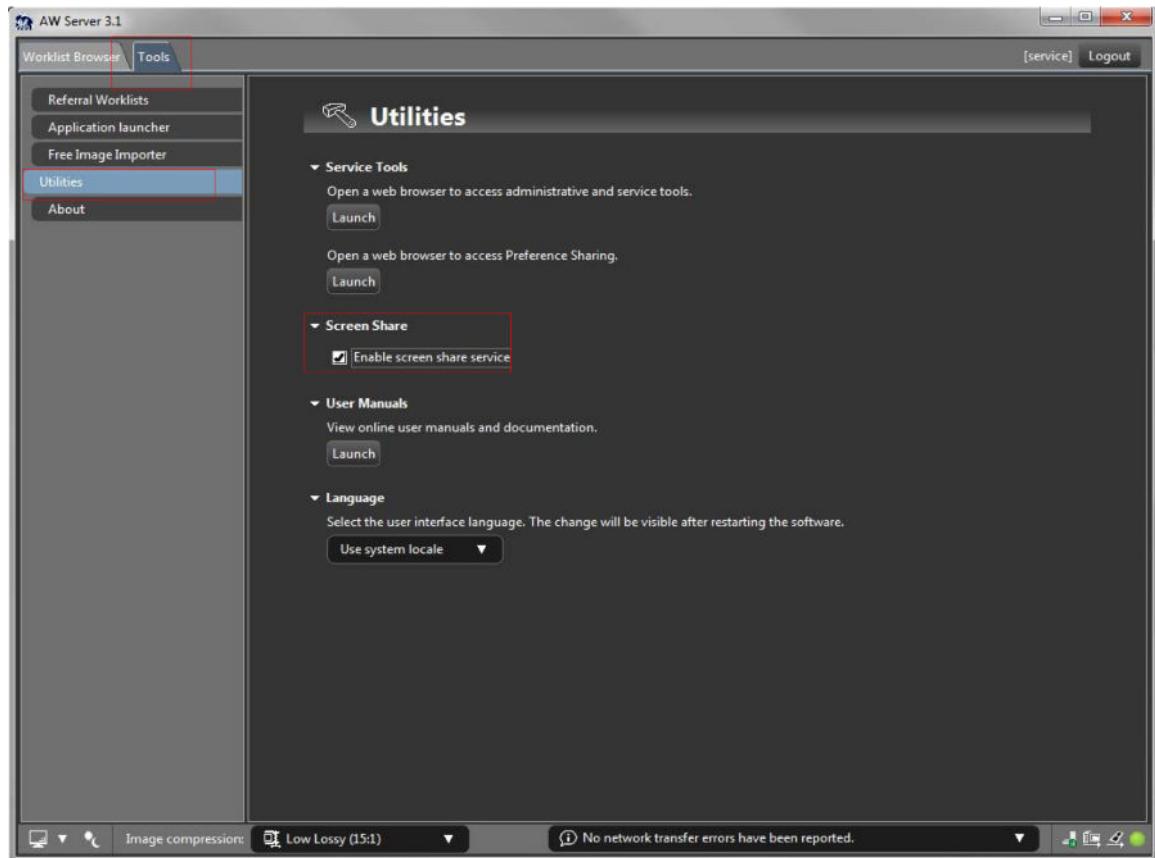
https://127.0.0.1:port#

port# is from **10000**.
 - c. Add several IP address (at least 5) with the hostname and different ports number as there can be several connections to the AW Server.
 - For instance, for InSite connectivity: **https://G5ZZ3QF2E:9300**; **https://G5ZZ3QF2E:9301...**
 - For instance, for RSvP connectivity: **https://127.0.0.1:10000**; **https://127.0.0.1:10001...**
 - d. Select **OK** and close the Java Control Panel.
2. In **Control Panel > Java > Advanced**, uncheck **Use SSL 2.0 compatible ClientHello format** and check **Use TLS 1.2** (should already be the case in default Java 7 and 8 JRE install).

3.3.4.2 Screen Sharing Scenario 1

3.3.4.2.1 Customer side

1. The customer having problems with the AWS application calls the support center remote engineer.
2. The service engineer asks the customer to share screen from **Tools > Utilities > Screen Share**:

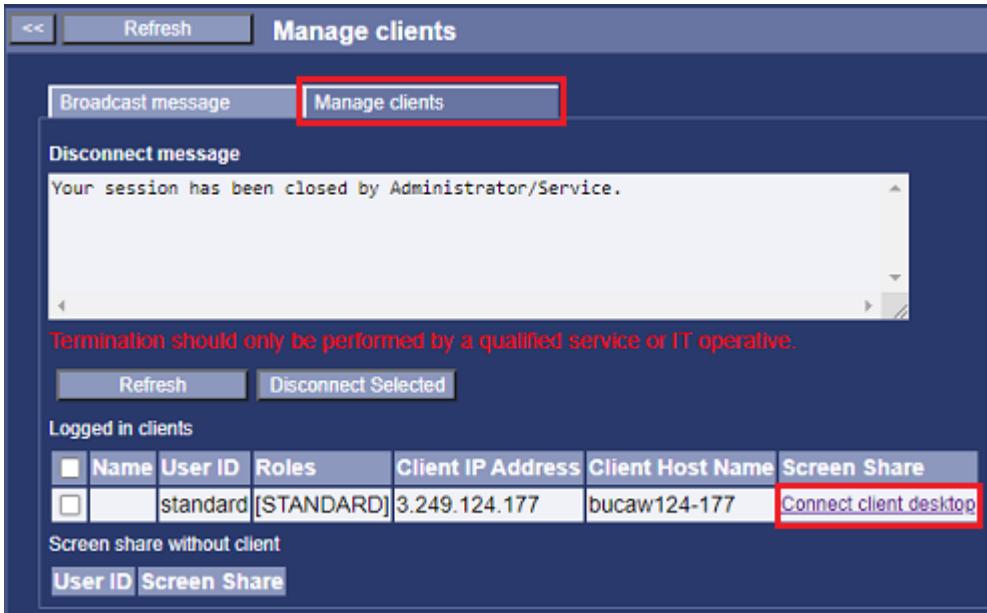


3. In **Tools > Utilities > Screen Share**, the customer checks the **Enable screen share service** checkbox.

3.3.4.2.2 Remote Service Engineer side

1. Remotely through FFA, start the Service Tool using the FFA connectivity tool, as described in [3.3.2 Accessing Service Tools from FFA on page 145](#).
2. Log into the Service Tools.
3. In **Administrative > Utilities > Clients**, select the *Manage Client* tab.

4. Click on **Connect client desktop** in the *Screen Share* column of the *Logged in clients* table.



The client desktop appears in a new tab or window.

5. If pop-ups related to the security certificate appear, accept the risk and acknowledge them.

From this point, the system behaves the same way as a regular VNC access. Remote Service Engineer can follow (view) the customer's workflow leading to the problem, and/or take full control of the customer's client PC.

Remote Engineer can investigate the whole login session. When investigating, the following items can be checked:

- Characterizing the problem: scenario to reproduce the problem, error messages returned by the AW Server Client, version of software used...
- Investigating possible root cause: network connectivity issue (using ping and Windows command line), mismatch between AW Server and AW Server Client, non-supported screen resolution...
- Providing a solution, which might include update of the PC configuration, up to reinstallation or upgrade of the AW Server Client.

The customer can stop Screen Sharing, which disconnects all connected participants.

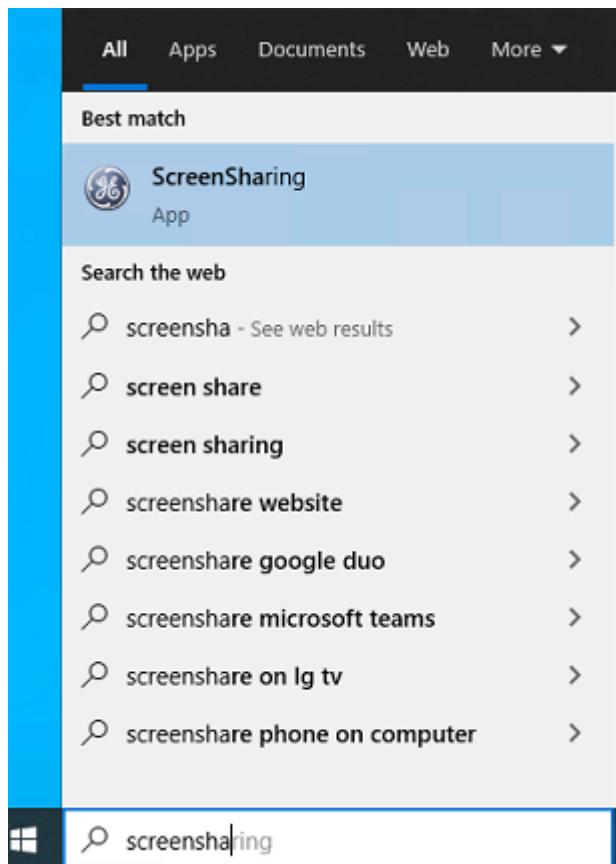
3.3.4.3 Screen Sharing Scenario 2

3.3.4.3.1 Customer side

The customer can't login and/or start the AWS application.

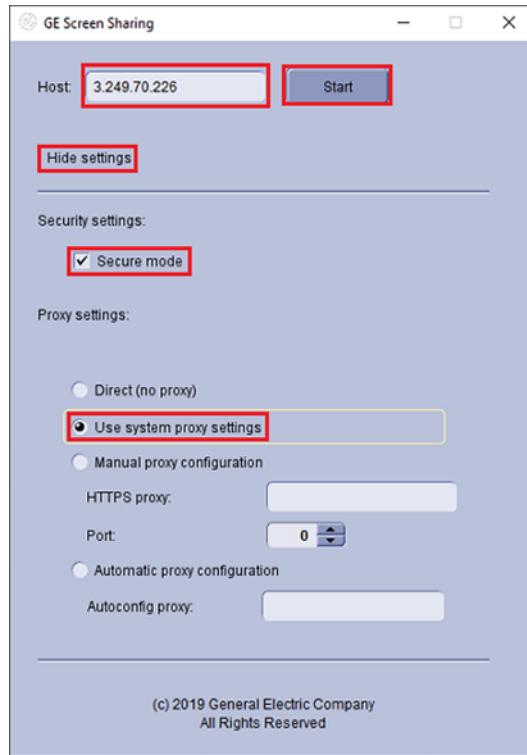
1. The customer having problems with the AWS application calls the support center remote engineer.

2. The customer starts ScreenSharing directly from Windows by typing **screensharing** in the search field.



3. Enter the IP address of the AW Server in the **Host** field.
4. Expand settings by selecting **Show settings**. Then check **Secure mode** and select **Use system proxy settings**.

5. Click on **Start** button.



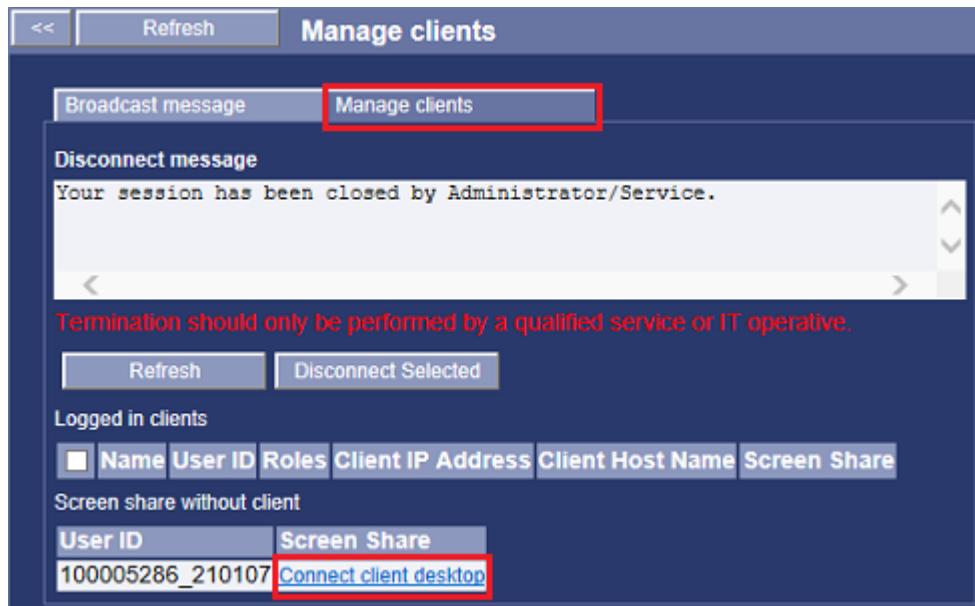
After successful start, the customer User ID is automatically provided by the system, aggregated from the User name (who logged into the Windows PC) and date and time:

E.g: aws_100122 for January 22, 2010.

3.3.4.3.2 Remote Service Engineer side

1. Remotely through FFA, start the Service Tool using the FFA connectivity tool, as described in [3.3.2 Accessing Service Tools from FFA on page 145](#).
2. Log into the Service Tools.
3. In **Administrative > Utilities > Clients**, select the *Manage Client* tab.

4. Click on **Connect client desktop** in the *Screen Share* column of the *Screen share without client* table.



The client desktop appears in a new tab or window.

5. If pop-ups related to the security certificate appear, accept the risk and acknowledge them.

From this point, the system behaves the same way as a regular VNC access. Remote Service Engineer can follow (view) the customer's workflow leading to the problem, and/or take full control of the customer's client PC.

Remote Engineer can investigate the whole login session. When investigating, the following items can be checked:

- Characterizing the problem: scenario to reproduce the problem, error messages returned by the AW Server Client, version of software used...
- Investigating possible root cause: network connectivity issue (using ping and Windows command line), mismatch between AW Server and AW Server Client, non-supported screen resolution...
- Providing a solution, which might include update of the PC configuration, up to reinstallation or upgrade of the AW Server Client.

The customer can stop Screen Sharing, which disconnects all connected participants.

3.4 General Troubleshooting

This section contains “general” troubleshooting information for the AW Server.

NOTE

Additional Troubleshooting information will be provided by Service Note. Please check availability of Service Notes for the AW Server 3.2 Product Line in your GE Healthcare Documentation Portal.

Information is provided in the following categories:

- Section [3.4.1 Understanding the HealthPage on page 154](#)
- Section [3.4.2 Basic User Troubleshooting Tips on page 167](#)
- Section [3.4.3 Troubleshooting AW Server Platform / Application Error Messages on page 177](#)
- Section [3.4.4 Troubleshooting Seamless Integration on page 183](#)

- Section [3.4.5 Tools and tips on page 186](#)
- Section [3.4.6 AW Server workarounds on page 213](#)
- Section [3.4.7 Troubleshooting applications and licenses on page 259](#)
- Section [3.4.8 Cybersecurity support on page 270](#)

3.4.1 Understanding the HealthPage

HealthPage is a diagnostic status tool. It is the first item on the menu, and is also the page that displays automatically when the user goes into Service Tools.

The HOME page of the ServiceTools is the server HealthPage. It provides a pictorial and data snapshot of the fundamental components of the SERVER: **CONFIGURATION** status, **HARDWARE / VIRTUAL MACHINE** Status, and **SOFTWARE** status.

The tool was designed for several purposes:

- Provide a snapshot glimpse of the server's overall functional status and configuration.
- Monitor server hardware and provide visual status alerts, or monitor the resources attributed to the virtual machine and provide visual status alerts.
- Provide a status for the primary software processes and services of the server and the ability to restart them when necessary.

There are FIVE sections on the server HealthPage:

Hardware Subsystem & Status / Virtual Machine & Status

System Configuration

Version information

Configuration & Status

Software Subsystem

Software Subsystem essential for Service Tools

The **RESTART** button restarts all AWS software processes in their required order — except the processes needed to support the Service Tools.

NOTICE

POTENTIAL LOSS OR CORRUPTION OF DATA. RESTARTING THE SOFTWARE SUBSYSTEM APPLICATIONS / SERVICES SHOULD ONLY BE PERFORMED BY A QUALIFIED SERVICE OR IT OPERATIVE. The Restart option is designed to perform an orderly shutdown and startup of all of the AW Server software processes — a system "**warm-reboot**" so to speak. The tool will present the user with a warning about continuing while not in Maintenance Mode — because this action **WILL DISCONNECT ALL USERS**.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take. Reference the maintenance mode in the SERVICE section of this document before activating this function.

NOTICE

FREQUENTLY use the **Refresh / Refresh all** buttons for each section of the HealthPage, to get the latest status. It can take up to a few minutes for the HealthPage to load completely or to refresh... During this time certain sections or fields may not display data or updated data. Other operations can still be performed.

SERVICE TOOLS HealthPage example (NON-VIRTUALIZED AW Server HOSTED on HP server)

The screenshot shows the Service Tools HealthPage for a non-virtualized AW Server hosted on an HP server. The page is divided into several sections:

- Hardware Subsystem:** A table showing status for Temperature (OK), Fan Status (Not critical), Voltage (Not applicable), Power Status (Not critical), UPS Status (Not applicable), and RAID Status (OK). A red arrow points from the 'Not applicable' entries to the text "Warning - Normal display condition for HP Servers".
- System Configuration:** A large table with many rows of system information. A red arrow labeled "Warning" points to the "Image partition next file system check date" row, which shows "Sat Jan 20 19:10:49 2019".
- Version Information:** A table showing AWS build date (20190111), AWS version (aws-3.2.3-2-1902.5-975c1d6d), and various software versions for EA3, EAT, Nuevo, CoLA, Service Tools, and ICM.
- Configuration and status:** A section with "Pull from system" and "Display" buttons. Below it is a table for the Software Subsystem, which includes rows for Image Management Subsystem (nuevo) (OK), Firewall (pnf) (Failed), Audit Server (eat) (OK), Authentication/Authorization Server (ea3) (OK), Application interoperability platform (dotmed) (OK), Super Server (aweservice) (OK), Client exporting subsystem (rmp-server) (OK), Built-in License Server (cola) (Unused), Secure Direct Connect (secure_dc) (OK), Printing Service (prserver) (OK), Preprocessing (xpreproc) (OK), Integration Service (pacointeg-webservice) (OK), Time Server (ntpd) (OK), DICOM Direct Connect (tomcat-local) (OK), Smart Card Login (tomcat-smartcard) (OK), Media Creator (mediacreator-app) (OK), and Configuration Service (configuration-service) (OK). A red arrow points from the "Failed" status to the text "Firewall turned off considered as error".
- Software Subsystem essential for Service Tools:** A table showing the status for httpd (OK), tomcat (OK), rmiregistry (OK), servicermi (OK), and awsservicermi (OK).

Annotations in red text are overlaid on the screenshot:

- "Warning - Normal display condition for HP Servers" (points to the 'Not applicable' rows in the Hardware Subsystem table).
- "Warning" (points to the "Image partition next file system check date" row in the System Configuration table).
- "Firewall turned off considered as error" (points to the "Failed" status in the Software Subsystem table).

- In the example above (for a non-virtualized AW Server), the HealthPage reports errors (in RED) and warnings (in Yellow)
- RAID status failed: Error can be reported on the images disk array (RAID status).

- PNF Firewall failed: The AWS software considers as an error condition the firewall when turned off.
- Image partition mount count: Close to the maximum before Filesystem check will be launched

NOTE

For the HP servers, the Fan status, Power status and Voltage information may not fully available, so this “normal behavior” will be displayed in yellow as a warning. However, when any of these devices fail, status will display in RED.

NOTE

Other small differences to the information captured on the HealthPage may occur, depending on the server configuration.

3.4.1.1 Hardware Subsystem

Hardware failures for the High Tier server are dispatched to the vendor for final analysis and resolution.

GEHC Service (local or remote) is tasked to capture failed hardware sensor information and to dispatch it according to the Hardware Break / Fix process detailed in Chapter 1, [1.4 Service Model and Break-Fix Processes on page 46](#) of this document. There are TWO Service actionable tools included in the Healthpage interface:

1. Sensor Details

- This is a non-invasive tool used to query the status of the hardware elements that IPMI tool software is configured to monitor.
- IPMI (**Intelligent Platform Management Interface**) defines a set of common interfaces to computer hardware and firmware, which system administrators can use to monitor system health and manage the system.

The SENSOR DETAILS tool is setup to capture the current status of the server hardware (except DISK DRIVES) based on the native values and specifications that are in the current implementation of the IPMI standard when this product was released. It is conceivable that a BIOS or OS update to the system might change these standards and break part or all of this "Healthpage" sensor details implementation. **The implementation may or may not get updated when or if this happens.** This could result in false-positive indications, or false negative indications.

FOR NON-VIRTUALIZED SYSTEMS IT IS RECOMMENDED TO CONFIRM READINGS WITH THE COMMAND-LINE IPMITOOL SENSOR SCRIPT AND THE SERVER'S ILO WEB INTERFACE.

- To access the ipmitool utility via command-line, type in **ipmitool <Enter>** for a list of available command options and switches. Please note that this command works only after the AW Platform is loaded.
- **Use the command-line IPMI tool (ipmitool sensor) to confirm or over-rule HealthPage sensor details.** Reference the figure below for a screenshot of the HealthPage sensor details.
- Also use the service processor “iLO” hardware sensor tool (**System Monitoring**) to verify or double-check hardware status, if iLO is applicable ([A.4 WGET on page 470](#)).

In any case, if still not sure, the Vendor Break/Fix model can be initiated, and the Vendor will make the final determination, and confirm whether or not the IPMI standard has changed, or if there is a hardware fault... Reference the break/fix process information in the **SERVICE** section of this document.

Sensor Details:

- Click on the **Sensor Details** button under the *Hardware Subsystems Status* table.

A window will pop-up displaying a table of hardware sensors. This table may require that you scroll your browser window down in order to view all of it. Additionally, there is a **Cancel** button at the bottom of the window to exit the display.

The primary elements that the healthpage Hardware Subsystem monitors are:

- Temperature
 - All the various temperature status sensors are combined into this element. **If ONE or more of them turn to a failed status, this element will show a RED Failure indication.** Clicking on the sensor details button will show the particular failure(s).
 - **Exception – The sensors that monitor CPU Temperature are designed to automatically shut the system down if they fail. This is normal, and is a safety precaution.**
 - **If the server keeps shutting down, will not boot-up, will not accept a load-from-cold, and/or indicates a CPU malfunction – this is obviously a significant hardware failure and should be dispatched to the Vendor for resolution via the break/fix model referenced in the SERVICE section of this document.**
- Fan Status
 - All the various fan status sensors are combined into this element. **If ONE or more of them turn to a failed status, this element will show a RED Failure indication.** Clicking on the sensor details button will show the particular failure(s).
- Voltage
 - All the various voltage status sensors are combined into this element. **If ONE or more of them turn to a failed status, this element will show a RED Failure indication.** Clicking on the sensor details button will show the particular failure(s).
 - **If the server keeps shutting down, will not boot-up, will not accept a load-from-cold, and/or indicates a Voltage malfunction – this is obviously a significant hardware failure and should be dispatched to the Vendor for resolution via the break/fix model referenced in the SERVICE section of this document.**
- Power Status
 - All the various power status sensors are combined into this element. **If ONE or more of them turn to a failed status, this element will show a RED Failure indication.** Clicking on the sensor details button will show the particular failure(s).
 - **If the server keeps shutting down, will not boot-up, will not accept a load-from-cold, and/or indicates a Power malfunction – this is obviously a significant hardware failure and should be dispatched to the Vendor (High Tier server case) for resolution via the break/fix model described at Chapter 1, [1.4 Service Model and Break-Fix Processes on page 46](#).**
- UPS Status
 - If the UPS driver is not installed, the status displays Not applicable on yellow background.
 - If the UPS driver is installed and running, the status displays OK on green background.
 - If the UPS driver is installed but is not running, the status displays Failed on red background.

NOTE

Sensor details status indication can also be CR for critical or NC for non-critical.

NOTICE

Information about the sensor data table elements:

- The **SENSOR DETAILS** listed in the pop-up table — **do not include RAID / Disk Drive information — RAID / Disk drive status and error information is reported separately.**
- Some of the elements are reported in degrees, rpm, volts, and have OK or Fail indicators. These are easy to understand. But some have "discrete" hexadecimal indicators. These are subjective to the current implementation of the standard.
- Additionally, some of the elements are not supported at present, and are denoted as na (not applicable).

Explanation of sensor value columns - Example below is for a Non-virtualized AW Server hosted on an HP Server:

- 1st column is the sensor name
- 2nd column is the reading
- 3rd column is the metric of the 2nd column.
- 4th value is the status related to this value ok, error, critical, not critical (nc), not applicable (na).
- 8th and 9th column is the lower and upper specification limit if present.

Figure 3-7 HARDWARE SUBSYSTEM SENSOR DETAILS

Check Power Supply and Fans status on Service Processor page								
Sensor Type	Value							
Power Supply 1	105.000	Watts	nc	na	na	na	na	na
Power Supply 2	100.000	Watts	nc	na	na	na	na	na
Fan Block 1	6.664	unspecified	nc	na	na	na	na	na
Fan Block 2	6.664	unspecified	nc	na	na	na	na	na
Fan Block 3	6.272	unspecified	nc	na	na	na	na	na
Fan Block 4	31.360	unspecified	nc	na	na	na	na	na
Fan Block 5	31.360	unspecified	nc	na	na	na	na	na
Fan Block 6	31.360	unspecified	nc	na	na	na	na	na
01-Inlet Ambient	24.000	degrees C	ok	na	na	na	42.000	46.000
02-CPU 1	40.000	degrees C	ok	na	na	na	70.000	0.000
03-CPU 2	40.000	degrees C	ok	na	na	na	70.000	0.000
04-CPU 3	40.000	degrees C	ok	na	na	na	70.000	0.000
05-CPU 4	40.000	degrees C	ok	na	na	na	70.000	0.000
06-P1 DIMM 1-6	34.000	degrees C	ok	na	na	na	87.000	0.000
07-P1 DIMM 7-12	34.000	degrees C	ok	na	na	na	87.000	0.000
08-P2 DIMM 1-6	36.000	degrees C	ok	na	na	na	87.000	0.000
09-P2 DIMM 7-12	35.000	degrees C	ok	na	na	na	87.000	0.000
10-P3 DIMM 1-6	31.000	degrees C	ok	na	na	na	87.000	0.000
11-P3 DIMM 7-12	32.000	degrees C	ok	na	na	na	87.000	0.000
12-P4 DIMM 1-6	35.000	degrees C	ok	na	na	na	87.000	0.000
13-P4 DIMM 7-12	32.000	degrees C	ok	na	na	na	87.000	0.000
14-HD Max	35.000	degrees C	ok	na	na	na	60.000	0.000
15-Chipset	50.000	degrees C	ok	na	na	na	105.000	0.000
16-P/S 1	31.000	degrees C	ok	na	na	na	0.000	0.000
17-P/S 2	31.000	degrees C	ok	na	na	na	0.000	0.000
18-P/S 2 Zone	35.000	degrees C	ok	na	na	na	75.000	80.000
19-VR P1	39.000	degrees C	ok	na	na	na	115.000	120.000
20-VR P2	42.000	degrees C	ok	na	na	na	115.000	120.000
21-VR P3	38.000	degrees C	ok	na	na	na	115.000	120.000
22-VR P4	39.000	degrees C	ok	na	na	na	115.000	120.000
23-VR P3 Zone	32.000	degrees C	ok	na	na	na	80.000	85.000
24-VR P1 Mem1	30.000	degrees C	ok	na	na	na	115.000	120.000

2. RAID Status

This HealthPage sensor element is designed to report the status of the RAID / Disk Drive Subsystems.

- For the HPE ProLiant DL580 G7 Server / HPE ProLiant DL560 Gen8 Server High tier, it monitors the `/var/log/hp-snmp-agents/cma.log` for **failures of either of the TWO RAID Controllers**.
- For the HP Low Tier server and the HPE ProLiant DL360 Gen10 Server / HPE ProLiant DL360 Gen9 Server, it monitors the `/var/log/hp-snmp-agents/cma.log` for **failures of the 2 system disks / controller and the image data disks / controller**.

The RAID status can take one of the following values:

- OK: no issues with the logical drives
- Degraded: there is a disk failure, however the logical drives are still available. In this case, it is URGENTLY needed to replace the failed disk.
- Failed: there are several disks failures, resulting in one or more logical drives being unavailable. In this case, it is URGENTLY needed to replace the failed disk.
- Recovering: the logical drives are being rebuilt.

When the RAID controller is Degraded or Failed the AW Server **HealthPage > Hardware Subsystem > RAID Status** turns **RED**, and displays a general context of the error or status change. When the RAID controller is in Recovering, the RAID status is displayed in **YELLOW** in Healthpage.

When this happens — the `/var/log/hp-snmp-agents/cma.log` (HP) should always be accessed to confirm the issue, and acquire the device and serial number details of the involved drive(s).

- Go to the **Log Viewer - `/var/log/hp-snmp-agents/cma.log`** file (HP server) OR
- Open up the **Terminal Tool** in the **Tools** menu, login and enter the command:
`more /var/log/hp-snmp-agents/cma.log <Enter>` (HP server)
 (use the space bar to page to the date and time and error in question)

NOTE

Refer to [3.7.5 HPE ProLiant DL560 Gen8 Server troubleshooting tips on page 307](#) and [3.8.5 HPE ProLiant DL580 G7 Server troubleshooting tips on page 313](#) for more details on identifying drive details.

3. Refresh button

When clicking on this button, a message **Checking** will display in yellow color, followed by the message **Success** displayed in green color, and the display will be refreshed.

NOTE THE ERROR/STATUS INFORMATION, AND RELAY IT TO THE VENDOR VIA THE VENDOR HARDWARE BREAK / FIX PROCESS (**HIGH TIER SERVER CASE**) DESCRIBED IN [1.4 Service Model and Break-Fix Processes on page 46](#) OF THIS DOCUMENT.

ALL HIGH TIER SERVER HARDWARE ISSUES ARE DISPATCHED TO THE VENDOR FOR RESOLUTION.

Once this disk error information is captured, and forwarded to the Vendor for service - there is no need for any further hardware trouble-shooting by GEHC until the Vendor resolves the issue.

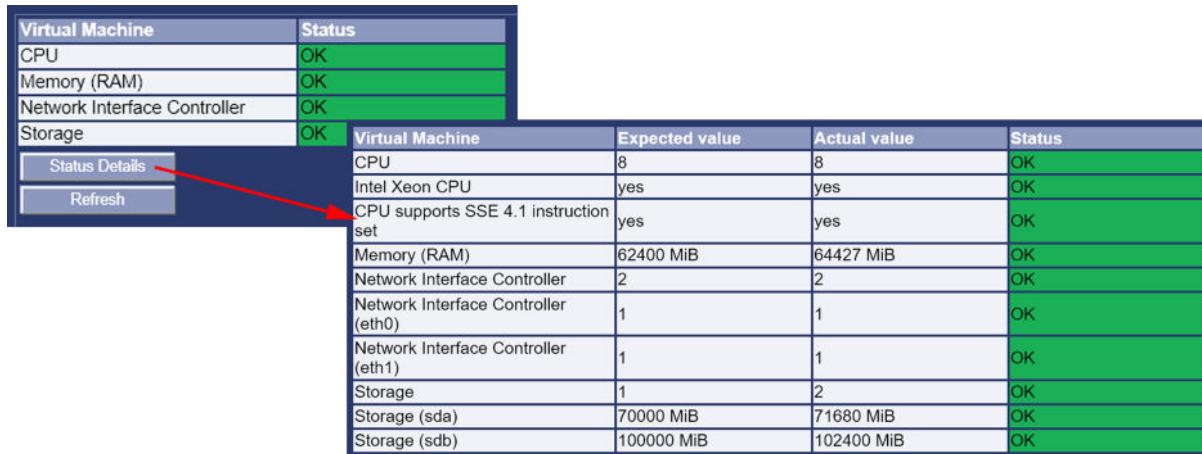
ALL IMAGE DATA DISK DRIVES should be left on site for customer disposition.

The Hardware Subsystem **RED** error information will automatically clear after the new disk drive(s) have been installed, and have completely rebuilt into their respective mirrored-set(s) — **REFRESH** the browser...

New disk drives automatically will be “scrubbed” or rebuilt into their mirrored-set. This progress can be monitored in `/var/log/hp-snmp-agents/cma.log` (HP server).

3.4.1.2 Virtual Machine Status

This section of the HealthPage replaces the Hardware Status section on a virtualized AW Server (hosted on a Virtual Machine). An example is shown below.



The screenshot shows two tables. The top table is a summary of virtual machine components and their status. The bottom table is a detailed view of the CPU hardware resource, showing its configuration and status.

Virtual Machine	Status
CPU	OK
Memory (RAM)	OK
Network Interface Controller	OK
Storage	OK

Virtual Machine	Expected value	Actual value	Status
CPU	8	8	OK
Intel Xeon CPU	yes	yes	OK
CPU supports SSE 4.1 instruction set	yes	yes	OK
Memory (RAM)	62400 MiB	64427 MiB	OK
Network Interface Controller	2	2	OK
Network Interface Controller (eth0)	1	1	OK
Network Interface Controller (eth1)	1	1	OK
Storage	1	2	OK
Storage (sda)	70000 MiB	71680 MiB	OK
Storage (sdb)	100000 MiB	102400 MiB	OK

- Click on the **Status Details** button to display details of the *virtual* hardware resource configuration and status, as shown in the example above.

NOTE

For Virtual machines, the HealthPage checks the key minimal requirements. It does not give the status of the underlying physical hardware.

3.4.1.3 System Configuration

This section of the HealthPage is common to both virtualized and non-virtualized AW Servers, with a few minor differences in the values that can be returned.

- System ID** - Version prior to AW Server 3.2 Ext. 4.2: This is the service system ID — manually entered in the Initial Configuration Device data page.
- System ID (CRM Number)** - From version AW Server 3.2 Ext. 4.2: This is the service system ID and the CRM Number — manually entered in the Initial Configuration Remote Service RSvP page. This is a unique machine identifier for the GE Backoffice.
- Platform Version**: The platform software build name and version.
- Hostname / IP Address**: Refer to the rules in the AW Server 3.2 Installation and Service Manual, Specific field - Characters rules and limitations when setting the hostname during the network configuration.
- DICOM Hostname / AET / Port** - Version prior to AW Server 3.2 Ext. 4.2: DICOM Hostname (or Application Entity Title) is same as the Host Name and the port is 4006.
- Encrypted (TLS) AET / Port** - From version AW Server 3.2 Ext. 4.0: Encrypted Application Entity Title and port is 2762.
- Plain AET / Port** - From version AW Server 3.2 Ext. 4.0: Application Entity Title and port is 4006.
- CPU (x)**: Server CPU hardware specs - the number of cores appears in brackets. For a virtualized AW Server this shows the configuration of virtual CPU allocated to the VM.
- Operating System**: Linux build name.
- OS Version**: Version level of the Linux operating system.
- Modality OS Version**: Version of the AW Server OS.

- UDI: Value of the Unique Device Identifier. UDI is also stored in configuration file and is displayed in the AW Server home page. The UDI is an identifier for the platform software. There is no UDI for Applications or hardware.
- REF: Medical Device Item Number.
- LOT: Medical Device Production Control.
- Uptime: Amount of time the server has been up since last reboot.
- Memory Total / Free: Amount of memory detected in the server. For a virtualized AW Server this shows the configuration of virtual memory allocated to the VM.
- OS Disk Space Total / Free: Capacity of the "system" disk(s) partition(s), and amount of current free space available. TURNS RED WHEN <10%. For a virtualized AW Server this shows the configuration of virtual disk space allocated to the VM.

This free space data status can differ from the df -h command-line values, due to the fact there are different approaches to free space analysis. The one used here is the closest to how the AWS software subsystem estimates the free space).

- Image Disk Total / Free: Capacity of Image disk(s) partition(s), and amount of current free space. TURNS RED WHEN <5%
- Backup Disk Space / Free: Capacity of the dedicated backup disk partition, and amount of free space. TURNS RED WHEN <5%
- Log Disk Space / Free: Capacity of the dedicated log disk partition, and amount of free space. TURNS RED WHEN <10%
- Network Queue Status: Summary of the DICOM queue status from the **Administrative > Utilities > Network Queue** page. TURNS YELLOW OR RED WHEN ACTIVE OR THERE ARE QUEUE FAILURES...
- Auto Delete (High / Low): displays the high and low mark values when turned on.
- Delete option for worklist browser: displays the current setting (on/off) of the Delete option to allow the user to perform data deletions from the worklist browser.
- Image partition Mount count (Current / Max.): displays the current number of mounts and the maximum number of mounts “allowed” before an automatic filesystem check will be launched at next reboot. Turns yellow when close to maximum.
- Image partition next file system check date: displays the date after which an automatic filesystem check will be launched at next reboot. Turns yellow when close to date.

NOTICE

Anticipate the automatic filesystem check routine start, so that it does not launch when you are on-site performing maintenance tasks. The filesystem check is a time-consuming process (up to several hours) during which access to the AW Server system is totally disabled. See [A.13 Filesystem Check on page 500](#) for details.

- Signer certificate expiration date: displays the date until the Signer's certificate is valid. AW Server's digital certificate has been signed with this certificate. This field is displayed with a green background normally and displayed with a yellow background when the expiration date is close.
- Certificate expiration date: displays the date until which the digital certificate is valid. After this date, the AWS Clients will display a pop-up for invalid certificate at each login. This field is displayed with a green background normally and displayed with a yellow background when the expiration date is close. If the field is yellow, follow instructions in [2.4.1.1 Certificate](#)

[Management on page 76](#) and [A.21 Installing/renewing an AW Server external CA signed certificate on page 514](#) to renew the certificate.

- Generic mode – Clam AV Antivirus Software status: if the Clam AV Antivirus is activated, this field displays Activated on white background, otherwise it displays Not activated on white background.
- RMF mode – McAfee Antivirus Software status: if Secured for RMF mode is activated, this field displays Activated in green background.
- Machine type: e.g: ProLiant DL580 G7 for a non-virtualized server, or Virtual Platform for a virtualized server.
- Install mode: This value is always set to server for AW Servers.
- DICOM AET(printing): The DICOM Application Entity Title of your AW Server
- Service Processor : The IP address of the iLO Service processor you have entered during the *Initial Configuration* steps.
- InSite Checkout ID - Version prior to AW Server 3.2 Ext. 4.2: The System ID for remote connectivity, entered during the *Initial Configuration* steps if applicable.
- License ID: The system's licenseID.
- Integration: The system's integration mode.
- Cluster mode: Whether the system is currently declared as part of a server cluster (True or False).
- Registration status: Current supported values are Permanent or Invalid. Permanent is displayed on a green background and is a valid status. To set the registration key, go to the **Maintenance > Configuration Registration** menu.
- Registration key: Displays the registration key if it is installed. Displays InvalidKey otherwise.
- Automatic Configuration Status Summary: Status is Pass, if the AW Server has been configured using the Installation Wizard (Cloud-init mechanism). Otherwise it is N/A.
- Secured for RMF: Status is **ON** on yellow background, if the Secured for RMF mode has been activated. And the status is **ON, verified** on a green background if the RMF mode has been activated and verified. Otherwise it is **OFF**.
- RMF activation date: Date of the Secured for RMF mode activation.
- RMF verification date: Date of the Secured for RMF mode verification.

3.4.1.4 Version Information

This section of the HealthPage is common to both virtualized and non-virtualized AW Servers. It displays release details of the main software components installed.

3.4.1.5 Configuration and Status

This section of the HealthPage is common to both virtualized and non-virtualized AW Servers, with a few minor differences in the values that can be returned.

Pull from system

- Click on the **Pull from System** button, to download the configStatus zipped file to your Personal computer. Use this to obtain the latest Config after each update to the server, and then send it to the Back Office. (Refer to chapter 5, [5.3.8 Registration on page 429](#)).

Display

- Click on the **Display** button, to display the configStatus file in a new web page.
- Click on the **Hide** button when done, to close the window.

3.4.1.6 Software Subsystem

The **Software Subsystem** lists the status of the primary software services that run the AW Server Application:

- **GREEN** — the service is running correctly.
- **RED** — the service has failed or is not running correctly.
- Be careful for any RED indications. Some of the services are not essential core AW Server operation services. For instance, the *Client Exporting subsystem*. This service could be failing, but will likely not impact the overall operation of the server. This could affect the way you approach trouble-shooting...
- **GRAY** — the service is not configured or being used — for instance, if the built-in license server is not being used.

NOTE

In the case of a **RED** Failure indication, there are at least FOUR potential actions that can be taken to attempt to resolve the issue.

1. Investigate the corresponding error log information, which may contain the details of the failure, and lead to a resolution activity.
 - Most of the services listed in the subsystem have parenthetical names after them — Super Server (**aweservice**).
 - **This name corresponds to an identical parenthetical name after its error-log name in the Log Viewer Tool (Diagnostic > Log Viewer). The apache, tomcat, rmiregistry, and awsservice items are needed to run the tool, so if they are bad you will likely not be able to view the Service Tools at all.** Regardless, the error logs for these are named the same as the service...
2. It might be necessary to **Restart** the services to reset non-fatal failing software service(s). In this case it is similar to doing a reboot of the system, only it is only rebooting the AW Server Software System.

There are also TWO command-line scripts that can be used to restart the software services:

- /usr/share/ServiceTools/scripts/healthpage/**restart_st.sh**
 - /usr/share/ServiceTools/scripts/healthpage/**restart_all.sh**
- (the "**Restart**" button is mapped to this script)

3. Performing a system reboot is also a potential action.
4. If all other actions are not successful — and there is no apparent hardware failure - and there is a suspicion that the software is at fault — a load-from-cold re-install can be performed.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

3.4.1.7 Software Subsystems "CORE" Services

- Image Management (nuevo)
- Firewall (pnf)
- Audit Server (eat)

- Authentication/Authorization Server (ea3)
- Application interoperability platform (dotmed)
- Super Server (aweservice)
- Client Exporting subsystem (rmpserver)
- Built-in License Server (cola)
- Secure Direct Connect (secure_dc)
- Printing Service (prserver)
- Pre-processing (xpreproc)
- Integration Service (pacsinteg-webservice)
- Time Server (ntpd)

NOTE

The complete name of the *dotmed* service is "dotmedservice" and the complete name of the *tomcat* service is "tomcat6"

- DICOM Direct Connect (tomcat-local)
- Smart Card Login (tomcat-smartcard)
- Media creator (mediacreator-app)
- Configuration Service (configuration-service)

3.4.1.8 Software Subsystem Restart

The “Restart” button shuts down and restarts the entire software subsystem.

When clicking on the **Restart** button, the following message is displayed:

“The system is not in maintenance mode. Do you want to continue?

NOTICE

Potential loss or corruption of data.

RESTARTING THE SOFTWARE SUBSYSTEM APPLICATIONS / SERVICES SHOULD ONLY BE PERFORMED BY A QUALIFIED SERVICE OR IT OPERATIVE.

The Restart option is designed to perform an orderly shutdown and startup of all of the AW Server software processes — a system "**warm-reboot**" so to speak. The tool will present the user with a warning about continuing while not in Maintenance Mode — because this action **WILL DISCONNECT ALL USERS**.

Reference the maintenance mode in the SERVICE section of this document before activating this function.

Recommendation:

One way to determine whether this type of intervention is appropriate or not is to weigh the impact of the failure against the number of users currently using the system. If the impact of the failure is that the system is essentially down anyway, then restarting all or rebooting the server is a no risk activity. However, if the failure has not put the system out of use, and there are several users currently using the system successfully — then you may want to forgo the action for now, or plan the activity for a predetermined time via the maintenance mode tool. See the SERVICE section of the document.

This warning also applies to the command-line restart scripts:

- /usr/share/ServiceTools/scripts/healthpage/**restart_st.sh**

- /usr/share/ServiceTools/scripts/healthpage/restart_all.sh

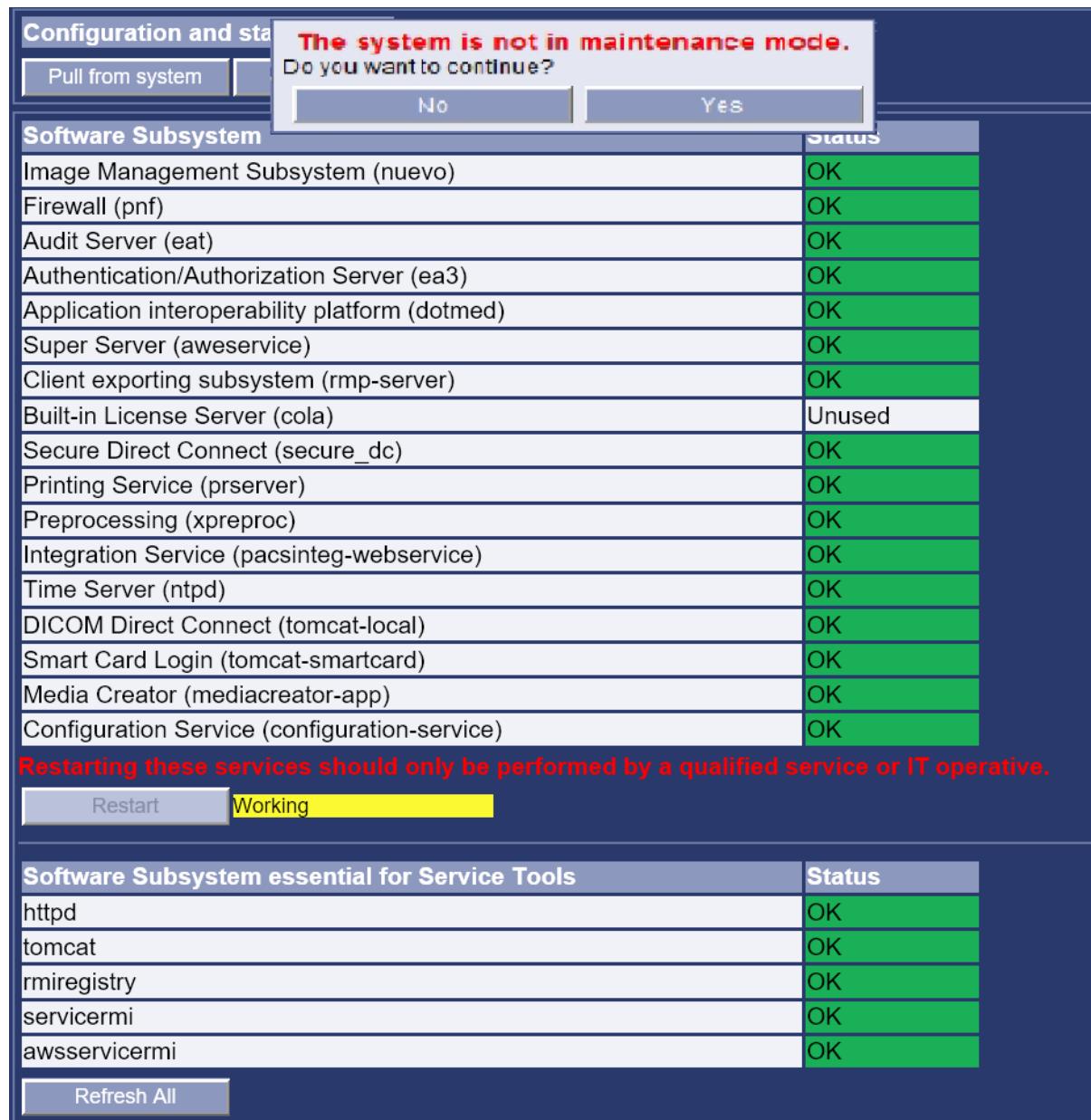
NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

NOTE

There is a watchdog service running in the background. It checks regularly for the core services. If any services are not running and no client is logged in, it will attempt to restart the service(s). In case of Cola server, the service is restarted only in the case of the internal Cola server

Figure 3-8 HEALTHPAGE SOFTWARE RESTART TOOL



- **Software Subsystem Restart Process** — Click on the **Restart** button beneath the Software Subsystem status table. A message will pop-up indicating the system is not in maintenance mode, all users will be disconnected, and do you want to proceed. **Reference the Maintenance Mode detail in the SERVICE section of this document.** If you wish to proceed without first

initiating the maintenance mode, click OK. Otherwise, go to the maintenance mode tool, and then come back to this tool when directed to.

- A yellow message ("Working" ; "Success") will indicate that the **services are being restarted — please wait**. After roughly 2 minutes, when complete, the message will switch to **Loading... Please Wait**. This means the healthpage is refreshing / loading. After a minute or so, the healthpage will display, and if the restart was successful, all the software services will indicate OK — except if the cola service is not being used. If not, you will need to pursue the steps listed above for **RED** failure indications...

NOTE

The following services are not restarted by the procedure above: ntpd and pnf.

3.4.1.9 Software Subsystems Essential for Service Tools

- Httpd (needed to run Service tool)
 - CORE Service
- Tomcat (needed to run Service tool)
 - CORE Service
- Rmiregistry (needed to run Service tool)
 - CORE Service
- Servicermi (needed to run Service tool)
 - CORE Service
- Awservicermi (needed to run Service tool)
 - CORE Service

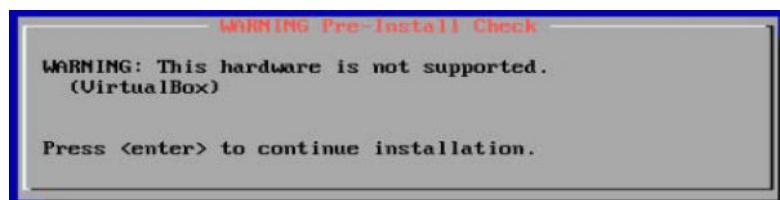
NOTE

The HealthPage is the first step in the server stand-alone diagnostic . After completing all the above analysis, sensor details, and potential restart — go to the **Diagnostic > Test > Server** — tool to perform the final step, testing the SERVER as a stand-alone device.

3.4.1.10 Hypervisor hardware not supported

Refer to the AW Server 3.2 Pre-Installation Manual, Requirements for Virtual AW Server to know the virtualization platforms (hypervisors) supported by the AW server.

At time of the virtual AW Server creation, the following or similar message may be displayed, to warn that the hypervisor type on which the VM for AW Server is being created is not supported.



Even though not validated, it is allowed to create a virtual AW Server on this type of hypervisor. In that case, the HealthPage displays a warning message such as shown in the below example.

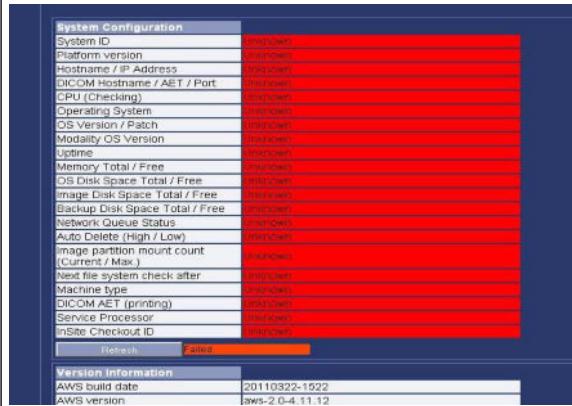
As a consequence of hypervisor not supported, erratic behavior might occur with the virtual AW Server.

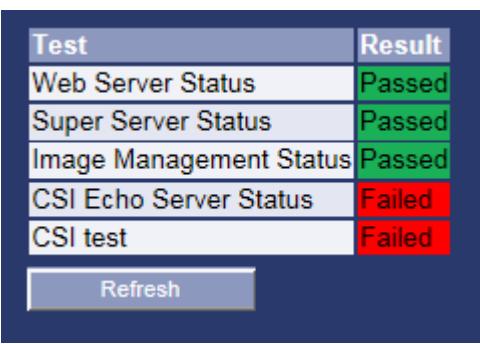
(Current / Max.)	Value
Image partition next file system check date	Not applicable
Certificate expiration date	Mon 02 May 2022 11:07:54 AM CEST
Clam AV Antivirus Software status	Not activated
Machine type	VirtualBox VirtualBox 5.0.24 Unsupported version!
Install mode	server
DICOM AET (printing)	
Service Processor	N/A
InSite Checkout ID	
License ID	2fd5a23f
Integration	No integration
Cluster mode	False
Registration status	Invalid
Registration key	InvalidKey

3.4.2 Basic User Troubleshooting Tips

Problems (non-exhaustive)	Solutions
<ul style="list-style-type: none"> Server webpage cannot be reached Application cannot be launched via client Service Tools cannot be accessed 	Potential power outage / restore or attached storage array hardware / software issue.
Cannot log in.	Re-enter the user name or password. Both are case sensitive.
Log in failed due to user account error.	Check that user is set up either as local or enterprise user.
Cannot see all the system tools.	Standard users see only a limited set of tools. Users with administrator privileges see more tools.
Get the following message: Login Failed IP address is not an AW Server	<ul style="list-style-type: none"> Verify and retype the IP address. Check network connection.
Can't connect. Get the following message: Connection failed for unknown reason	Verify IP address and re-type the user name and password.
Cannot open ZIP Files Generated by AW Server.	Try using another archive tool, such as 7-Zip.
Undesired logout/disconnection from AWCCT website with Internet Explorer.	To prevent these disconnections from AWCCT Website, perform the following: <ol style="list-style-type: none"> On your Windows task bar, select the Internet Explorer shortcut. Right click on the shortcut and select "Start InPrivate Browsing". A new Internet Explorer window will open. Use the newly opened window to access AWCCT website. There should be no more disconnections. While using the InPrivate Browsing mode, your navigation history, cookies and temporary files will not be kept.
KVM displays warning message. The KVM displays the following warning message after launching startx command: Warning message Current resolution is not supported Reverting to best display setting.	Hit any of the buttons below the KVM screen to hide the error message.
Server memory not sufficient for platform configuration. When applying the platform configuration, the following message is displayed: Slice-count license could not be activated. Server memory is not sufficient.	Check the memory currently available and ensure it is the appropriate amount for your hardware and your platform license. See 2.3.8 Platform Configuration on page 62 . If your memory configuration is less than required, order replacement parts for memory modules, see Ordering Replacement Parts .

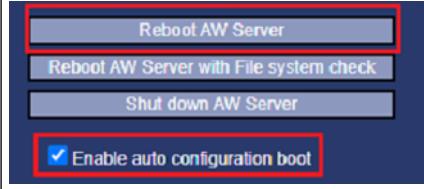
Problems (non-exhaustive)	Solutions
<p>AW Server boot failure after OS load.</p> <p>After OS load, the following error message is displayed quickly while booting:</p> <p>ERST: Failed to get Error Log address Range</p> <p>After this message, the HELiOS boot screen displays normally, then the following error message displays and the server freezes:</p> <p>Kernel panic - not syncing/ Attempted to kill init !</p>	<p>Check if there are any USB device connected to the AW Server, if so remove them and perform a Load From Cold to reinstall correctly the OS.</p> <p>Alternatively, the KVM switch can cause this issue. In this case, unplug the KVM and perform a Load From Cold using iLO.</p>
<p>Load Analyzer tool usage.</p> <p>The tool can be used to collect or analyze system component logs, in case of application starting performance problems. The tool is currently only supported for Seamless integration mode. No results will be collected if the AWS is in Standalone or Hybrid integration mode.</p>	<p>Create <code>/tmp/app_load_logs.zip</code> archive with all the necessary files for later analysis:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root 2. Launch the following command: <code>loadanalyzer -a -o /tmp/app_load_logs.zip</code> <Enter> <p>The zip archive can be copied and sent to Engineering team for analysis.</p>
<p>Maximum number of licenses exceeded.</p>	<p>The AW Server has 2, 4 and 8 seat license options (corresponding to 8000, 16,000, 40,000, 80,000 and up to 160,000 slices configuration). If concurrent users attain the maximum number of licenses or the number of slices, additional users must wait until someone logs off before they can sign in. To diagnose the issue, use Diagnostic > Floating License.</p>
<p>Application could not be started.</p>	<ul style="list-style-type: none"> • Each client can run a maximum of 3 applications. Close one of the applications to continue. • Log out and log back in. Wait approximately 30 seconds before trying to start application from desktop.
<p>The connection to the server has been closed.</p>	<ul style="list-style-type: none"> • System was inactive for a predetermined time set by the administrator Network connection failed. • Network connection failed.
<p>Cannot save data to the server.</p>	<p>There is not enough free space on the server.</p> <ul style="list-style-type: none"> • System Administrator may need to delete data on the server. • Contact GE Service to configure the Auto delete feature which automatically deletes old images from the server database.
<p>System is slow.</p>	<ul style="list-style-type: none"> • Check network connection and bandwidth. • Verify the network latency is less than identified in data sheet. • Run the Network Analyzer tool. • Check compression ratio. • Check that PC meets minimum requirements.
<p>Application cannot be launched via the client and you do not receive any message.</p>	<p>Check the amount of RAM on your client. The application will not start with insufficient RAM.</p>

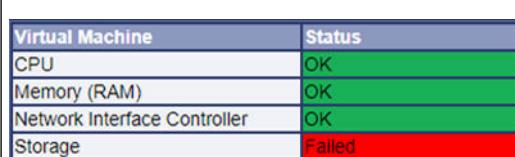
Problems (non-exhaustive)	Solutions																																																				
Unable to connect to the AW Server or start applications when connecting from outside the local network, i.e.VPN.	<p>VPN or hospital security is rejecting AW Server network traffic for security reasons. Attempt to fix this by turning on the AW Server security layer on the client.</p> <ul style="list-style-type: none"> On the AW Server Client login page, check the box Secure mode. Using the Secure mode slows down system performance. OR, the site VPN solution may not be compatible with AW Server functionality. 																																																				
<p>User can log in to the AW Server and preview images, but 2D Viewer, 3D viewer, and other advanced applications will not start.</p> <p>In addition, a message similar to the following may display:</p> <pre><date.....><NX proxy info.....>Server was not able to compose sdc_selection file based on the given selection data!</pre>	<p>The 2D/3D viewer application uses X Windows terminal software.</p> <p>You may already have other X Windows terminal software on your PC that provides the ability to run and display UNIX applications (X clients) from the MS Windows environment. Such tools include, but are not limited to, Exceed and CygwinX.</p> <p>They can be used on the local PC to:</p> <ul style="list-style-type: none"> - Access applications and information running on network hosts - Establish simultaneous connections to different computers running X clients <p>Use any appropriate window manager to preserve familiarity with the PC or X environment.</p> <p>Furthermore, if the X Windows is CygwinX, when the AW Client exits, it also kills the previously existing X server and all its running applications.</p> <p>To avoid this error, the user must exit any X Windows applications before starting the AW Server client (directly or via integration) on the PC.</p>																																																				
<p>All system configuration information is displayed in RED in the HealthPage.</p>  <table border="1"> <thead> <tr> <th colspan="2">System Configuration</th> </tr> </thead> <tbody> <tr><td>System ID</td><td>XXXXXXXXXX</td></tr> <tr><td>Platform version</td><td>XXXXXXXXXX</td></tr> <tr><td>Hostname / IP Address</td><td>XXXXXXXXXX</td></tr> <tr><td>DICOM Hostname / AE/T / Port</td><td>XXXXXXXXXX</td></tr> <tr><td>CPU (Checking)</td><td>XXXXXXXXXX</td></tr> <tr><td>Operating System</td><td>XXXXXXXXXX</td></tr> <tr><td>OS Version / Patch</td><td>XXXXXXXXXX</td></tr> <tr><td>Modality OS Version</td><td>XXXXXXXXXX</td></tr> <tr><td>Uptime</td><td>XXXXXXXXXX</td></tr> <tr><td>Memory Total / Free</td><td>XXXXXXXXXX</td></tr> <tr><td>OS Disk Space Total / Free</td><td>XXXXXXXXXX</td></tr> <tr><td>Image Disk Space Total / Free</td><td>XXXXXXXXXX</td></tr> <tr><td>Backup Disk Space Total / Free</td><td>XXXXXXXXXX</td></tr> <tr><td>Network Queue Status</td><td>XXXXXXXXXX</td></tr> <tr><td>Auto Delete (High / Low)</td><td>XXXXXXXXXX</td></tr> <tr><td>Image partition mount count (Current / Max.)</td><td>XXXXXXXXXX</td></tr> <tr><td>Next file system check after</td><td>XXXXXXXXXX</td></tr> <tr><td>Machine type</td><td>XXXXXXXXXX</td></tr> <tr><td>DICOM AET (printing)</td><td>XXXXXXXXXX</td></tr> <tr><td>Service Processor</td><td>XXXXXXXXXX</td></tr> <tr><td>InSite Checkout ID</td><td>XXXXXXXXXX</td></tr> <tr><td>Reboot</td><td>XXXXXX</td></tr> <tr><td colspan="2">Version Information</td></tr> <tr><td>AWS build date</td><td>20110322-1522</td></tr> <tr><td>AWS version</td><td>aws-2.0-4.11.12</td></tr> </tbody> </table>	System Configuration		System ID	XXXXXXXXXX	Platform version	XXXXXXXXXX	Hostname / IP Address	XXXXXXXXXX	DICOM Hostname / AE/T / Port	XXXXXXXXXX	CPU (Checking)	XXXXXXXXXX	Operating System	XXXXXXXXXX	OS Version / Patch	XXXXXXXXXX	Modality OS Version	XXXXXXXXXX	Uptime	XXXXXXXXXX	Memory Total / Free	XXXXXXXXXX	OS Disk Space Total / Free	XXXXXXXXXX	Image Disk Space Total / Free	XXXXXXXXXX	Backup Disk Space Total / Free	XXXXXXXXXX	Network Queue Status	XXXXXXXXXX	Auto Delete (High / Low)	XXXXXXXXXX	Image partition mount count (Current / Max.)	XXXXXXXXXX	Next file system check after	XXXXXXXXXX	Machine type	XXXXXXXXXX	DICOM AET (printing)	XXXXXXXXXX	Service Processor	XXXXXXXXXX	InSite Checkout ID	XXXXXXXXXX	Reboot	XXXXXX	Version Information		AWS build date	20110322-1522	AWS version	aws-2.0-4.11.12	<p>Refer to the rules in the AW Server 3.2 Installation and Service Manual, Specific field - Characters rules and limitations to set the hostname during the network configuration.</p>
System Configuration																																																					
System ID	XXXXXXXXXX																																																				
Platform version	XXXXXXXXXX																																																				
Hostname / IP Address	XXXXXXXXXX																																																				
DICOM Hostname / AE/T / Port	XXXXXXXXXX																																																				
CPU (Checking)	XXXXXXXXXX																																																				
Operating System	XXXXXXXXXX																																																				
OS Version / Patch	XXXXXXXXXX																																																				
Modality OS Version	XXXXXXXXXX																																																				
Uptime	XXXXXXXXXX																																																				
Memory Total / Free	XXXXXXXXXX																																																				
OS Disk Space Total / Free	XXXXXXXXXX																																																				
Image Disk Space Total / Free	XXXXXXXXXX																																																				
Backup Disk Space Total / Free	XXXXXXXXXX																																																				
Network Queue Status	XXXXXXXXXX																																																				
Auto Delete (High / Low)	XXXXXXXXXX																																																				
Image partition mount count (Current / Max.)	XXXXXXXXXX																																																				
Next file system check after	XXXXXXXXXX																																																				
Machine type	XXXXXXXXXX																																																				
DICOM AET (printing)	XXXXXXXXXX																																																				
Service Processor	XXXXXXXXXX																																																				
InSite Checkout ID	XXXXXXXXXX																																																				
Reboot	XXXXXX																																																				
Version Information																																																					
AWS build date	20110322-1522																																																				
AWS version	aws-2.0-4.11.12																																																				
<p>The AW Server Hostname is displayed in red in the HealthPage.</p>	<p>Refer to the rules in the AW Server 3.2 Installation and Service Manual, Specific field - Characters rules and limitations to set the hostname during the network configuration.</p>																																																				
<p>Healthpage displays nuevo image disk space query failed.</p> <p>After first boot of an AW Server, the HealthPage displays an error for image disk size. Image Disk Space Total is displayed as Unknown in red.</p>	<p>Reboot the AW Server to solve this issue. Refer to 2.5.3 Shutdown / Reboot on page 96 for more details.</p>																																																				

Problems (non-exhaustive)	Solutions												
Anti-virus or security software installed on the client workstation's host operating system (Windows) may cause problems with the AW Server client and/or Universal Viewer client (depending on integration mode).	See 3.4.5.15 Windows Anti-virus / Security Software on the Client Workstation on page 206 in this chapter.												
Partition is full / problems sending or receiving images to PACS.	<p>Check disk file usage of logfiles (in particular check the <code>/var/log/gehc/sdc/logfiles</code> directory). Also refer to 3.2.3 Log Files Viewer on page 126.</p> <ol style="list-style-type: none"> After a database recovery, the following folder may contain many images, causing disk availability issues on the partition. Open the AW Server Console/terminal and type: <pre>cd /export/home1/sdc_image_pool <Enter> cd failed_to_reinstall <Enter></pre> To check the utilization of this folder type: <pre>du -sk . <Enter></pre> According to the results (displayed in kb), you may reinstall, delete, or simply leave the images as they are. Reinstallation is normally recommended - contact your OLC for details. 												
<p>Platform Configuration is invalid in Finish maintenance menu.</p> <p>In Service Tools, in Maintenance > Maintenance > Finish Maintenance, the Platform Configuration status is displayed as Invalid in red.</p>	Go to Initial Configuration > Platform Configuration and apply the platform license key by clicking Next, Next again and Apply .												
<p>CSI Echo and Test failed in Diagnostic > Test > Server page.</p>  <table border="1" data-bbox="271 1147 703 1455"> <thead> <tr> <th>Test</th> <th>Result</th> </tr> </thead> <tbody> <tr> <td>Web Server Status</td> <td>Passed</td> </tr> <tr> <td>Super Server Status</td> <td>Passed</td> </tr> <tr> <td>Image Management Status</td> <td>Passed</td> </tr> <tr> <td>CSI Echo Server Status</td> <td>Failed</td> </tr> <tr> <td>CSI test</td> <td>Failed</td> </tr> </tbody> </table>	Test	Result	Web Server Status	Passed	Super Server Status	Passed	Image Management Status	Passed	CSI Echo Server Status	Failed	CSI test	Failed	<p>This indicator is only a testing signal. It does not break the installation procedure and does not causes problem in "good working" of the server.</p> <p>This problem is related to service naming in new OS and is fixed in AWS3.2 Ext.4.0.</p>
Test	Result												
Web Server Status	Passed												
Super Server Status	Passed												
Image Management Status	Passed												
CSI Echo Server Status	Failed												
CSI test	Failed												
<p>AW Server Client encounters performance issues on the client PC when Symantec Endpoint Protection is used.</p> <p>Symantec Endpoint Protection's Intrusion Prevention component intercepts data at the network layer and scans each network packets which might affect the interactive performance of the product negatively.</p>	<p>Configure the following, on "policy level" in Symantec, and in the priority order described in following points:</p> <ul style="list-style-type: none"> Exclude AW Server(s) from the Intrusion Prevention. OR, Enable Out-of-band scanning for the group of clients. OR, Remove Intrusion Prevention component from the workstations having AW Server Client. 												
<p>On AW Server 3.2 Ext. 3.4 (and prior versions), the configuration of the Advantage SIM Laser Marker failed in the Service Tools. The connection with the Lap Laser computer running on Windows 10 failed.</p> <p>The cause of the issue is that the SMBv1 Samba protocol running on the client computer with Windows 10 is disabled.</p>	<p>To avoid failure of the Advantage SIM Laser Marker configuration, SMBv1 Samba protocol should be enabled in client computer running on Windows 10. For full procedure refer to https://docs.microsoft.com/en-sg/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3.</p>												

Problems (non-exhaustive)	Solutions
<p>On AW Server 3.2 Ext. 3.4, the uninstallation of the Advantage SIM application, from the Service Tools, failed. The cause of the issue is that the uninstallation process tries to change the name of the uninstall script, but it has not the root privileges to perform the action. And so, the uninstall script is not found.</p>	<p>To avoid failure of the AdvantageSim uninstallation:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root. 2. Change the name of the uninstall script: <code>cd /export/home/sdc/install <Enter></code> <code>cp uninstall.awe uninstall.advsim <Enter></code> 3. Uninstall Advantage SIM application. However, no logs are displayed in the UI at this step. 4. Click on the Refresh button in the Version Management page. 5. The application is successfully uninstalled even if there is no message in the UI.
<p>On AW Server 3.2 Ext. 4.0, cannot save System Configuration Backup from Service Tools backup utility if Advantage SIM is installed. After AdvantageSim MD installation, a CUPS backup checkbox is created, added and selected in the backup list. When backing up the system configuration by clicking on Pull from system or Save on system, the backup fails with the message "Pre-backup script failed".</p>	<p>To avoid failure of the backup, unselect the CUPS backup checkbox, then back up the system configuration by clicking on Pull from system or Save on system. CUPS can be configured manually after restoring the system configuration if needed.</p>
<p>On AW Server 3.2 Ext. 4.0 and 4.2, in some cases the CardIQ Xpress Process 2.3 Ext. 6 application does not install correctly. This occurs if Advantage SIM 9.0 Ext. 5 application has been installed before CardIQ Xpress Process.</p>	<p>To avoid failure of the CardIQ Xpress Process installation, there are two options:</p> <p>Perform a Load From Cold to reinstall the OS and the AW Server.</p> <p>If the Load From Cold is not possible, follow the below steps:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root. 2. Uninstall Advantage SIM application using the following command: <code>/export/home/sdc/install/uninstall.advsim --complete <Enter></code> 3. Install CardIQ Xpress Process application from the Version Management page. 4. Install Advantage SIM application from the Version Management page.
<p>On the CT/MR/PET Consoles, the Solo Client (AW Server Client) crashes when changing from or to full screen mode several times and clicking in and outside the resize button.</p>	<p>Recommendation to avoid this issue:</p> <p>When changing from or to full screen mode, be sure to click on the resize button and not outside the resize button area. Or select the full screen/Restore button using the arrow on the right side of the resize button.</p>
<p>On the CT/MR/PET Consoles, the Solo Client (AW Server Client) displays irregular shaped viewports, in Volume Viewer, when switching between dual screen/single screen layouts.</p>	<p>Recommendation to avoid this issue:</p> <p>Switch from dual screen mode to single screen mode, only when the application protocol is already running.</p>

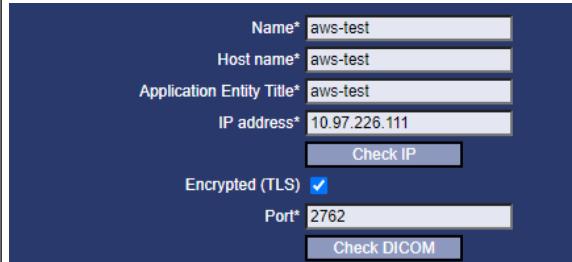
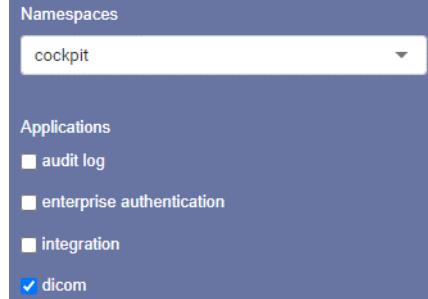
Problems (non-exhaustive)	Solutions
<p>Network Queue failure in the Service tools.</p> <p>The DICOM Network Queue management panel, available from Administrative > Utilities > Network Queue, does not work. Indeed, the DICOM SCU communication going out from AW Server are missing. As a consequence, the Network Queue Status, displaying a summary of the DICOM Network Queue in the HealthPage, is not accurate.</p>	<p>The missing information (history of DICOM SCU communication going out from AW Server) can be analyzed from the logfile <code>~sdc/nuevo/logfiles/serviceProvider.log</code> as follows:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root 2. Review the logfile with a text editor or send it to OLC for analysis. You can view it using the following command in the terminal (type the <Space> key to go to the next page): <pre data-bbox="859 512 1298 579"><code>cd ~sdc/nuevo/logfiles <Enter> less serviceProvider.log <Enter></code></pre>
<p>On AW Server 3.2 Ext. 4.0 and 4.2, in the Service tools Healthpage, the Automatic Configuration Status Summary status displays a Fail state.</p> <p>This occurs if the Enable auto configuration boot option is enabled (in the Tools > Reboot page) and the AW Server is rebooted (without being in the process of reenabling the Cloud-Init mechanism).</p>	<p>To recover the failed status in the Healthpage:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root and type the following command: <pre data-bbox="859 707 1362 774"><code>/root/provisioning/cicaws.py disable <Enter></code></pre> <ol style="list-style-type: none"> 2. On the Healthpage click on the Refresh button.
<p>During an upgrade from AW Server 3.2 Ext. 3.2 to Ext. 4.0 or up, in the Service tools Healthpage, the Registration Status and the Registration Key are invalid. Although, the Configuration Registration was successful and the Maintenance mode was turned off.</p>	<p>To recover the failed status in the Healthpage:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root. 2. Change the <code>/export/home/sdc/icm/resources/config</code> directory ownership: <pre data-bbox="859 983 1394 1051"><code>chown sdc:sdc -R /export/home/sdc/icm/ resources/config <Enter></code></pre> <ol style="list-style-type: none"> 3. Register again the AW Server configuration. Refer to Job Card IST013 in the AW Server 3.2 Installation Manual. 4. On the Healthpage check that the Registration Status and Key are valid.
<p>On AW Server 3.2 Ext. 4.0 and higher, when creating or updating a DICOM host, from the Service Tools in Administrative > Configuration > DICOM Hosts panel, an additional DICOM host with the same name ending with <code>_tmp</code> appears in the hosts list (for instance, when creating/updating the DICOM host "host1", another DICOM host named "host1_tmp" is created).</p> <p>This occurs only when the Name of the DICOM host is different than the Host name and when clicking on the Check DICOM button before applying the changes (before clicking on the Apply button).</p>	<p>To remove the additional DICOM host created (ending with <code>_tmp</code>), simply delete it:</p> <p>From the Service Tools in Administrative > Configuration > DICOM Hosts panel, select the DICOM host ending with <code>_tmp</code>, click on Delete button and acknowledge the popup that displays.</p>

Problems (non-exhaustive)	Solutions
<p>On AW Server 3.2 Ext. 4.2, some SmartScore result data series and reports are not automatically sent to the PACS when exiting the application.</p> <p>This occurs when the End of Review is configured with the Type of image set to generated, for the Host name selected (here the PACS).</p> <p>The cause of the issue is that SmartScore does not properly fill in the header of all the generated series.</p>	<p>To recover the missing SmartScore result data series and reports on the PACS, simply push/send them manually to the PACS, when possible depending on the integration mode.</p> <p>To avoid this issue to reoccur, for seamless and DDC integration modes only, set the Type of image to all for the PACS in the End of Review panel:</p> <p>From the Service Tools in Administrative > Configuration > End Of Review panel, set the Type of image to all for the Host name selected (here the PACS), then click on Apply button.</p> 
<p>On AW Server 3.2 Ext. 4.4, the service user cannot download any files provided by the Service tools: log files from the Log viewer, system configuration on the Healthpage, network capture with Network Analyzer.</p> <p>This occurs only after a backup is pulled from the system (from the Service Tools in Administrative > Backup > System configuration panel, by clicking on Pull from system) and if it is the first data downloaded on the system.</p> <p>In this case, the folder used to download the data (/tmp/download) is created with the wrong rights.</p>	<p>To recover from this issue and to avoid this issue to reoccur, restart the AW Server and download the configuration and status from the Healthpage, so that the download folder (/tmp/download) is created with the correct rights:</p> <ol style="list-style-type: none"> 1. Reboot the AW Server. Refer to 2.5.3 Shutdown / Reboot on page 96 for more details. 2. In the Healthpage, click on Pull from system below Configuration and status label to download the system configuration.
<p>On Nano-Cloud, depending on the Firefox version used, some features may not be available in the Service Tools.</p> <p>This occurs with the RSvP Configuration page that does not display when it is opened from Firefox on DB62 systems.</p>	<p>To remediate this issue, follow the below step:</p> <ol style="list-style-type: none"> 1. Open a new tab in Firefox and type in about:config to open the Firefox configuration page. 2. Set dom.moduleScripts.enabled property's value to false. 3. Close the tab.
<p>From AW Server 3.2 Ext. 4.0, the Automatic Configuration Status Summary status gets into failure in the Healthpage.</p>  <p>This occurs when activating the Enable auto configuration boot check box by mistake, from the Service Tools in Tools > Reboot panel, and after that, rebooting the AW Server.</p> 	<p>To recover the Automatic Configuration Status Summary status in the Healthpage:</p> <ol style="list-style-type: none"> 1. Open the AW Server Console/terminal, login as root. 2. Type the following command: <code>/root/provisioning/cicaws.py disable <Enter></code> 3. Refresh the Healthpage and check that the Automatic Configuration Status Summary status is N/A.

Problems (non-exhaustive)	Solutions
<p>The <code>/export/home1/sdc_image_pool/locks</code> directory contains the applications temporary lock files. This directory gets populated over time with these lock files when applications do not correctly clear the directory after running (at exit). This anomaly can lead to easily break the AW Server by preventing autodelete functionality over time and by making image partition filling up, and with that not allowing new image data arrival to the system.</p> <p>This issue is specifically present with SmartScore 4.0 application on AW Server 3.2. But it might occur with other application packages as well.</p>	<p>To recover the issue, remove the lock files from <code>/export/home1/sdc_image_pool/locks</code> directory:</p> <ol style="list-style-type: none"> Be sure that no user is using the system. Open the AW Server Console/terminal, login as root. Remove the lock files: <pre>rm -rf /export/home1/sdc_image_pool/locks/* <Enter></pre>
<p>From AW Server 3.2 Ext. 4.0 to Ext. 4.8, the file system check (fsck), while expired, does not run automatically upon reboot.</p> <p>The file system check expiration occurs while:</p> <ul style="list-style-type: none"> The number of time the system has restarted reaches the maximum number of restarts authorized without fsck. (The current date) – (the date of the last fsck) \geq the time authorized between two fsck. 	<p>To recover the issue, from the Service Tools select Tools > Reboot then click on Reboot AW Server with File system check button.</p>
<p>On AW Server 3.2 Ext. 4.4, when saving anonymous images from the Service Tools in Administration > Utilities > Image Database tool, the Service Tools crash with an “Unrecoverable error”.</p> <p>This occurs after a Load From Cold, if a backup file has been created. In this case, the temporary <code>/tmp/download</code> folder is created with wrong rights (<code>root</code> instead of <code>tomcat:tomcat</code>). As the Image Database tool uses this folder to save the images, it fails because it has not enough rights to write data in this folder.</p>	<p>To recover the issue:</p> <ol style="list-style-type: none"> Reboot the AW Server. Refer to 2.5.3 Shutdown / Reboot on page 96 for more details. <p>OR</p> <ol style="list-style-type: none"> Open the AW Server Console/terminal, login as root. <ol style="list-style-type: none"> Update the <code>/tmp/download</code> folder rights: <pre>chown tomcat:tomcat /tmp/download <Enter></pre> <p>OR</p> <ol style="list-style-type: none"> Delete the <code>/tmp/download</code> folder: <pre>rm -rf /tmp/download <Enter></pre>
<p>After finishing the Virtual AW server installation, the Storage section on the Service Tools Healthpage is red.</p>  <p>This occurs when the images partition (second virtual hard disk) is missing for Virtual AW Server in No-Integ (Standalone) or Hybrid mode.</p> <p>If the images partition (second virtual hard disk) is created post installation, the Storage status will turn green. However, the images partition will be created in a wrong place with a small capacity. So, images partition will be filled quickly.</p>	<p>To recover the issue:</p> <ol style="list-style-type: none"> Create the images partition (second virtual hard disk), if not already done. Refer to <i>Job Card IST001B</i> in the <i>AW Server 3.2 Installation Manual</i>. Perform a Load From Cold to reinstall the OS and the AW Server. Refer to <i>Job Card UPG001</i> in the <i>AW Server 3.2 Installation Manual</i>.

Problems (non-exhaustive)	Solutions
<p>In case of AW Server 3.2 Ext. 4.8 and Ext. 4.9 deployments where Edison Cockpit (Imaging Cockpit) is installed, the EAT Audit Trail logs related to the web-based AW Server Client (Web Client) and the next generation applications (CardIQ Suite) usage are not visible on the central log server after setting up Enterprise Repository with secure TLS connection e.g.: the selected Protocol is TLS IETF Syslog.</p>  	<p>NOTE</p> <p>This workaround only applies to AW server 3.2 Ext. 4.9.</p> <p>The issue cannot be fixed for AW Server 3.2 Ext. 4.8.</p> <p>To recover the issue:</p> <ol style="list-style-type: none"> 1. Make sure that you have set the Audit Source ID to the AW Server Host name. From the Service Tools, select Initial Configuration > Audit Trail (EAT) > Audit Message Settings, check the Audit Source ID. Refer to <i>Job Card IST008</i>, section <i>Audit Trail (EAT)</i> in the <i>AW Server 3.2 Installation Manual</i>. 2. From the Service Tools, select Configuration > Certificate Management > Trusted Certificates, and configure the CA certificate of the central log server for the edison-core Namespace. Refer to <i>Job Card IST010</i>, section <i>Associating a certificate with feature(s)</i> in the <i>AW Server 3.2 Installation Manual</i>. 3. Reboot the AW Server. From the Service Tools, select Tools > Reboot. 4. After performing steps 1 to 3, the EAT messages will be forwarded to the central log server. Due to a technical issue however the Audit logs related to the web-based AW Server Client (Web Client) and the next generation applications (CardIQ Suite) usage are slightly different from the Audit logs related to the legacy Solo client usage: the host name is different in the syslog header: <ul style="list-style-type: none"> - Audit logs related to legacy Solo client usage have the AW Server Host name in the syslog header. - Audit logs related to the Web Client and the next generation applications (CardIQ Suite) usage contain the Kubernetes pod name instead of the AW Server Host name. The pod name has the following pattern: <i>cp-eat-<random generated identifier></i> e.g.: <i>cp-eat-88b869c7f-mr52m</i> - Both type of Audit log messages do have the AW Server Host name in the XML payload inside the AuditSourceIdentification tag. Example of an Audit log related to legacy Solo client usage: <i>Dec 21 16:37:25 aws-test GE <?xml version="1.0" encoding="UTF-8"?><AuditMessage><EventIdentification</i>

Problems (non-exhaustive)	Solutions
	<p>EventActionCode="E" EventDate-Time="2022-12-21T15:37:25" EventOutcomeIndicator="0"><EventID csd-code="110114" codeSystemName="DCM" originalText="User Authentication"/><EventTypeCode csd-code="110122" codeSystemName="DCM" originalText="Login"/></EventIdentification><ActiveParticipant UserID="service" UserIsRequestor="true" NetworkAccessPointTypeCode="1" NetworkAccessPointID="localhost:4569"><RoleIDCode csd-code="110150" codeSystemName="DCM" originalText="Application"/></ActiveParticipant><ActiveParticipant UserID="CSI" UserName="AWS" UserIsRequestor="false" NetworkAccessPointTypeCode="2" NetworkAccessPointID="10.97.226.84"/></ActiveParticipant><AuditSourceIdentification AuditSourceID="aws-test"><AuditSourceTypeCode csd-code="9" codeSystemName="DCM" originalText="External source, other or unknown type"/></AuditSourceIdentification></AuditMessage></p> <p>Example of an Audit log message related to the Web Client and the next generation applications (CardIQ Suite) usage:</p> <pre>Dec 15 13:55:13 cp-eat-88b869c7f-mr52m GE <?xml version="1.0" encoding="UTF-8"?><AuditMessage><EventIdentification EventActionCode="R" EventDateTime="2022-12-15T13:55:13" EventOutcomeIndicator="0"><EventID csd-code="110103" codeSystemName="DCM" originalText="DICOM Instances Accessed"/></EventIdentification><ActiveParticipant UserID="EC Application Launcher" UserIsRequestor="true"/></ActiveParticipant><AuditSourceIdentification AuditSourceID="aws-test"><AuditSourceTypeCode csd-code="9" codeSystemName="DCM" originalText="External source, other or unknown type"/></AuditSourceIdentification><ParticipantObjectIdentification ParticipantObjectID="UNKNOWN" ParticipantObjectTypeCode="1" ParticipantObjectTypeCodeRole="1"><ParticipantObjectIDTypeCode csd-code="2" codeSystemName="RFC-3881" originalText="Patient Number"/><ParticipantObjectName/></ParticipantObjectIdentification><ParticipantObjectIdentification ParticipantObjectID="" ParticipantObjectTypeCode="2" ParticipantObjectTypeCodeRole="3"><ParticipantObjectIDTypeCode csd-code="110180" codeSystemName="DCM" originalText="Study Instance UID"/><ParticipantObjectName/></ParticipantObjectIdentification></AuditMessage></pre>

Problems (non-exhaustive)	Solutions																
<p>DICOM AET Port information (Encrypted (TLS) AET / Port and Plain AET / Port) on Service Tools Health-page, in the System Configuration section, shows incorrect information in certain integration modes (Hybrid, Seamless and DDC) where "N/A" value is displayed for Plain AET port.</p> <table border="1" data-bbox="239 399 790 467"> <tr> <td>Encrypted (TLS) AET / Port</td> <td>devaws-dpoc / 2762</td> </tr> <tr> <td>Plain AET / Port</td> <td>devaws-dpoc / N/A</td> </tr> </table>	Encrypted (TLS) AET / Port	devaws-dpoc / 2762	Plain AET / Port	devaws-dpoc / N/A	<p>Below is the correct information about the available DI-COM ports for the different configurations:</p> <table border="1" data-bbox="827 280 1435 527"> <thead> <tr> <th data-bbox="827 280 1013 348">Integration mode</th> <th data-bbox="1013 280 1235 348">Encrypted (TLS) AET / Port</th> <th data-bbox="1235 280 1435 348">Plain AET / Port</th> </tr> </thead> <tbody> <tr> <td data-bbox="827 348 1013 428">No-integ (Stand-alone), Hybrid</td> <td data-bbox="1013 348 1235 428">2762, 4020*</td> <td data-bbox="1235 348 1435 428">4006, 4010*</td> </tr> <tr> <td data-bbox="827 428 1013 473">Seamless</td> <td data-bbox="1013 428 1235 473">N/A</td> <td data-bbox="1235 428 1435 473">N/A</td> </tr> <tr> <td data-bbox="827 473 1013 527">DDC</td> <td data-bbox="1013 473 1235 527">4020**</td> <td data-bbox="1235 473 1435 527">4010**</td> </tr> </tbody> </table> <p>*Web Client is installed * and **Port is open for incoming DICOM associations, but any data pushed there without being requested by AW Server will be discarded. See latest revision of <i>5720690-1EN AW Server Conformance Statement for DI-COM</i> for further details.</p>	Integration mode	Encrypted (TLS) AET / Port	Plain AET / Port	No-integ (Stand-alone), Hybrid	2762, 4020*	4006, 4010*	Seamless	N/A	N/A	DDC	4020**	4010**
Encrypted (TLS) AET / Port	devaws-dpoc / 2762																
Plain AET / Port	devaws-dpoc / N/A																
Integration mode	Encrypted (TLS) AET / Port	Plain AET / Port															
No-integ (Stand-alone), Hybrid	2762, 4020*	4006, 4010*															
Seamless	N/A	N/A															
DDC	4020**	4010**															
<p>In case of AW Server 3.2 Ext. 4.8 and Ext. 4.9 deployments where Edison Cockpit (Imaging Cockpit) is installed, the remote DICOM host is not accessible via the web-based AW Server Client (Web Client) when the DICOM connection is set to Encrypted (TLS).</p>  <p>The following error message will appear when switching to the remote DICOM Host in the Web Client.</p> <p>"Worklist - Could not connect to data source. Retry your search. If the problem persists, please check with your system administrator."</p>  <p>3. Reboot the AW Server. From the Service Tools, select Tools > Reboot.</p>	<p>To recover the issue:</p> <ol style="list-style-type: none"> 1. Make sure that you have declared the AW Server on the remote DICOM host. Refer to <i>Job Card IST010</i>, section <i>Imaging Cockpit / AW Server Web Client</i> in the <i>AW Server 3.2 Installation Manual</i>. 2. From the Service Tools, select Configuration > Certificate Management > Trusted Certificates, and configure the CA certificate of the remote DICOM host for the cockpit Namespace. Refer to <i>Job Card IST010</i>, section <i>Associating a certificate with feature(s)</i> in the <i>AW Server 3.2 Installation Manual</i>. 																

3.4.3 Troubleshooting AW Server Platform / Application Error Messages

Source	Error	Cause	Resolution
Client Checker Tool	System requires resolution of 1024 x 768 to run the AW server, without which the images would appear distorted.		Change PC resolution (if graphics card allows)

Source	Error	Cause	Resolution
Client Checker Tool	System requires 1 GB of RAM to run the AW server, without which the performance will be degraded.		PC does not meet minimum RAM specifications
Client Checker Tool	System requires 1 GHz of CPU Speed to run the AW server, without which the performance will be degraded.		PC does not meet minimum CPU specifications
Client Checker Tool	System requires 24 Bit per pixel to run the AW server, without which the images would appear distorted.		Change PC resolution (if graphics card allows)
Client Checker Tool	AW System does not support this keyboard.		Use a different keyboard or select different locale on PC
Client Checker Tool	System requires temp directory free space of minimum (512 * 512 * 3000) to run the AW server, without which the performance will be degraded.		Delete temp files to free up space
Client Checker Tool	Monitor Quality Check failed.	Monitor quality test did not pass based on customer responses.	Local administrator should review results and adjust monitor settings so the test can pass.
Client Checker Tool	Basic System check failed	PC does not meet minimum specifications	Contact local administrator
Client start	client does not start OR client starts, but application does not start	Port conflict on the Windows client (some other software uses port 16131). Change the value:	<p>How to check the used ports:</p> <p>On Windows: http://www.petri.co.il/quickly_find_local_open_ports.htm</p> <p>On Linux: http://mylinuxnote-book.blogspot.com/2008/08/display-linux-open-ports-with-netstat.html</p> <p>Edit the <i>solo.ini</i> file on the client and change the value Dxwin.port=16131 to another suitable value.</p>
Copy/Paste or export of non DICOM image to client	Error, sending image to Remote Client	Image could not be sent from server to client	<ul style="list-style-type: none"> Attempt operation a second time Review <u>Platform: RMP Services log (rmpserver)</u> for potential root cause Restart AW Server Services from HealthPage (after confirming status of connected clients)
Copy/Paste or export of non DICOM image to client	Time out, sending image to Remote Client	Image could not be sent from server to client due to operation timeout	<ul style="list-style-type: none"> Attempt operation a second time Review Platform: RMP Services log (rmpserver) for potential root cause Ping client from server (or ping server from client) to ensure latency is not greater than 10ms
Display	East Asian languages are not properly displayed.	Regional settings	<p>Change the Language and Regional settings on the Client PC.</p> <ul style="list-style-type: none"> - Open the Control Panel - Select Regional and Language options - Click the boxes next to "Install files for complex script and right-to-left languages" and "Install files for East Asian languages".

Source	Error	Cause	Resolution
Service Tools (DICOM hosts)	Problem occurred during delete, unable to perform!	ServiceTool was unable to delete DICOM host	<ul style="list-style-type: none"> Review following logs for potential cause: <u>Platform: Nuevo - Service Provider process log (nuevo)</u> <u>Platform: Service Tools - servlet log</u> Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (DICOM hosts)	Problem occurred during query, unable to perform!	ServiceTool was unable to view DICOM host	<ul style="list-style-type: none"> Review following logs for potential cause: <u>Platform: Nuevo - Service Provider process log (nuevo)</u> <u>Platform: Service Tools - servlet log</u> Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (DICOM hosts)	Problem occurred during adding, unable to perform!	ServiceTool was unable to add DICOM host	<ul style="list-style-type: none"> Review following logs for potential cause: <u>Platform: Nuevo - Service Provider process log (nuevo)</u> <u>Platform: Service Tools - servlet log</u> Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (DICOM hosts)	Problem occurred during modifying, unable to perform!	ServiceTool was unable to modify DICOM host	<ul style="list-style-type: none"> Review following logs for potential cause: <u>Platform: Nuevo - Service Provider process log (nuevo)</u> <u>Platform: Service Tools - servlet log</u> Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (DICOM queue)	 WARNING you may need to refresh the list again in a few seconds to see the results of your actions.	Self-explanatory	Refresh list to see updates
Service Tools (Download Tool)	Error occurred during download.	The selected file was not able to download	<ul style="list-style-type: none"> Make sure file is still available in the AW Server file system Check to make sure web browser downloads are enabled Check site admin to see if downloads are blocked by local firewall Look in <u>Platform: Service Tools - servlet log</u> for potential root cause Restart AW Server Services from HealthPage (after confirming status of connected clients)

Source	Error	Cause	Resolution
Service Tools (general error messaging)	Unrecoverable error occurred! The UI has been disabled to avoid further operation!	This is displayed on the Service Tools Error page.	<ul style="list-style-type: none"> Logout of Service Tools and log back in Close web browser, open new web browser and log in
Service Tools (general error messaging)	Communication error occurred with the servlet.	An error occurred with ServiceTools software	<ul style="list-style-type: none"> Logout of Service Tools and log back in Close web browser, open new web browser and log in Restart AW Server services from HealthPage (after confirming status of connected clients)
Service Tools (general error messaging)	Unrecoverable error occurred during RMI communication!	Remote Message Invocation error	Restart RMI service <code>/etc/init.d/awsservicermi restart</code>
Service Tools (general error messaging)	Internal software error:	An error occurred with ServiceTools software	<ul style="list-style-type: none"> Logout of Service Tools and log back in Close web browser, open new web browser and log in Restart AW Server services from HealthPage (after confirming status of connected clients)
Service Tools (general error messaging)	The user is not authorized to perform the requested operation!	User does not have sufficient permission to execute a given function.	Log in as user with sufficient permission
Service Tools (Image Database tool)	Error occurred during database query, please find the server logs for details. Please refresh at exam level!	Database display did not refresh correctly.	<ul style="list-style-type: none"> Refresh again at exam level and then select the desired series or image Review following logs for potential cause: <u>Platform: Nuevo - Service Provider process log (nuevo)</u> <u>Platform: Service Tools - servlet log</u> Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (Image Database tool)	There was error during deletion of the DICOM objects having the following UIDs:	DICOM image could not be deleted.	<ul style="list-style-type: none"> Refresh image list to make sure image is still available for deletion Check Platform: Nuevo - Service Provider process log (nuevo) for root cause.
Service Tools (Image Database tool)	There was error during anonymization of the DICOM objects having the following UIDs:	DICOM image could not be anonymized	<ul style="list-style-type: none"> Refresh image list to make sure image is still available for anonymization Check Platform: Anonymizer log for root cause.
Service Tools (Login page)	The authenticated user does not have enough roles!	User does not have sufficient permission to execute a given function.	Log in as user with sufficient permission
Service Tools (Upload Tool)	The file specified does not exist or cannot be read!	The selected file on the client PC could not be accessed to upload to server.	Make sure the path and file name are correct and the file is still available for upload.
Service Tools (Upload)	Bad upload request.	There was an error uploading selected file to the server	<ul style="list-style-type: none"> Try again Make sure the path and file name are correct and the file is still available for upload.

Source	Error	Cause	Resolution
Service Tools (Upload)	Server could not write file!	File that operator attempted to upload could not be written to upload directory.	<ul style="list-style-type: none"> Try again Look in Platform: Service Tools - servlet log for potential root cause Restart AW Server Services from HealthPage (after confirming status of connected clients)
Service Tools (Upload)	Error occurred during upload:	There was an error uploading selected file to the server	<ul style="list-style-type: none"> Try again Make sure the path and file name are correct and the file is still available for upload. Look in Platform: Service Tools - servlet log for potential root cause. Check with local administrator to see if there is any firewall filters that could block upload. Restart AW Server Services from HealthPage (after confirming status of connected clients)
Volume Viewer	Connection to remote display cannot be established.	NX has tried and failed. This is displayed each time an NXproxy has failed to establish the connection with the NXagent, so the user might get this message multiple times. NX might still work (as 1 or 2 NX-es might be running)	<ul style="list-style-type: none"> Dismiss the message, and try to use the client anyway Try each of the following, in the order listed, to see if it fixes the problem: Logout/login, restart client, reboot, re-install client, call service. <p>NOTICE</p> <p>Before performing a shutdown or reboot, refer to 2.5.3 Shutdown / Reboot on page 96 for details of important precautions to take.</p>
Java Application (Client Checker, Pro-diag...)	Application is blocked when starting and the following message displays: "Application blocked by Security Settings" "Your security settings have blocked a self-signed application from running"	Java security settings do not allow execution of application that are self-signed.	<p>Create an exception rule for your server on your PC. Go to Control Panel>Java In the security tab, select "Edit Site List.." Click on "Add" and enter the IP address of your AW Server (e.g. "http://10.10.10.25", without the quotes) Select ok and close Java Control Panel.</p>

Source	Error	Cause	Resolution
Service Tools (Launch)	Service Tools access is blocked on Firefox with the following message: "Secure Connection Failed An error occurred during a connection to You have received an invalid certificate"	Certificate is invalid OR A previous certificate was saved in Firefox for the same IP address, then the AW Server was reinstalled or upgraded and a different certificate was automatically created during installation.	Check the validity of the certificate and re-install it OR Remove the previous certificate saved for this IP address and restart Firefox <ul style="list-style-type: none"> • In menu Options>Advanced>Certificates, select View Certificates • Identify the line with the IP address you are trying to access and select it. • Select Delete to delete the previous certificate. Close the Firefox tab and open a new tab. The regular certificate prompt will display.
Service Tools (Documentation)	In Service Tools Documentation > Documentation menu, when using Chrome, clicking "Documentation" only opens one documentation tab instead of two.	Chrome pop-up blocker is preventing the second documentation tab from opening	Go back to the Service Tools tab in Chrome, then click on the pop-up blocker icon at the top-right of the window. Select "always allow pop-ups from ..." OR Disable Pop-up blocker in Chrome Settings > Advanced Settings > Privacy > Content Settings, Pop-ups section.
Service Tools (Scalability)	HAPS health information does not appear in Scalability menu using IE web browsers.		"Display all websites in compatibility view" setting should be disabled in IE web browsers to display Service Tools pages appropriately.
Service Tools (Prodiag)	Prodiag page does not open in Chrome web browser.	Chrome does not support NPAPI plugins	Access the Prodiag page from Internet Explorer or Firefox browsers only.
Service Tools (Screen Sharing)	When trying to use screen sharing with Chrome, this message displayed from java in Chrome web browser: "The Chrome browser does not support NPAPI plug-ins and therefore will not run all Java content. Switch to a different browser (Firefox, Internet Explorer or Safari on Mac) to run the Java plug-in. More info"	Chrome 43 and 45 does not support NPAPI plugins which is required for java and this is used by screen share tool.	Access the Screen Sharing page from Internet Explorer or Firefox browsers only.
Service Tools (Screen Sharing & Prodiag)	Screen Sharing or Prodiag does not launch and returns an Application Error message: "ClassNotFoundException"	Java setting potentially incompatible with Secure Sockets Layer (SSL) or Transport Layer Security (TLS).	On the client PC, go to Control Panel > Programs > JAVA. In Java Control Panel, select the Advanced tab > Advanced Security Setting and disable "Use SSL 2.0 compatible ClientHello format".
Service Tools (Version Management)	It is not possible to select multiple files when using "upload DVD Collector" tool with Internet Explorer.	IE does not support multiple files upload	Use Firefox or Chrome to upload DVD Collector.
Service Tools (Web Client configuration & Register Configuration).	It is not possible to display the Web Client configuration page and the Register Configuration page is not fully functional with Internet Explorer.	IE does not support new features introduced on the UI of these external components.	Use Firefox or Chrome to view the Web Client configuration page and the Register Configuration page.

NOTE

The error messages in this section are indicative. New or altered messages may accompany future software releases.

3.4.4 Troubleshooting Seamless Integration

NOTE

In the case of issues with installation and configuration of the Universal Viewer client using CPACS or IW back end, always check the relevant sections of the related technical documentation (see **Chapter 8** for list of key related documents).

3.4.4.1 Preprocessing Issues

3.4.4.1.1 Symptoms

No auto-states are generated by Preprocessing, or Preprocessing is not launched.

3.4.4.1.2 Workaround

- In the Universal Viewer Site Configuration Tool, check the option "**Notification Enable**".
- Using the Integrad Control Panel, restart all services. Refer to the Universal Viewer Installation Manual.
- On the AW **Server's Service Tools > Initial Configuration > Integration**, verify that the connector plugin used is "Dakota Client Library" and not "Default Data Exchange"

3.4.4.2 Incompatible version of solomini (AWSERVER client)

In this case, you will normally be prompted to re-install a new version of the AWSERVER client.

3.4.4.3 Solomini not found

Verify that the installation has been done correctly on the client PC:

Launch 3D application from Universal Viewer or re-install AWSERVER client manually.

3.4.4.4 3D Applications Button Greyed Out

If the 3D Applications Button in the menu bar of the Universal Viewer client is greyed out, this indicates an integration issue. Check the following:

- In Service Tools, select **Initial Configuration > Integration**, verify that the connector plugin used is "Dakota Client Library" and not "Default Data Exchange"
- Universal Viewer: Check Integrad Control Panel, restart the Tomcat service (do this with extreme caution after customer agreement)
- IW Server Manager: Select **Web Server > System Services** to restart
- Universal Viewer Site Configuration Tool: Select **Info > AW Integration Wizard** and check the field entries for both tabs (in particular, check that the AWUSER has been created on the PACS). See the AW Server 3.2 Installation and Service Manual, Seamless integration - configuration steps on Universal Viewer Server for further details.

3.4.4.5 Display truncated when using dual screens

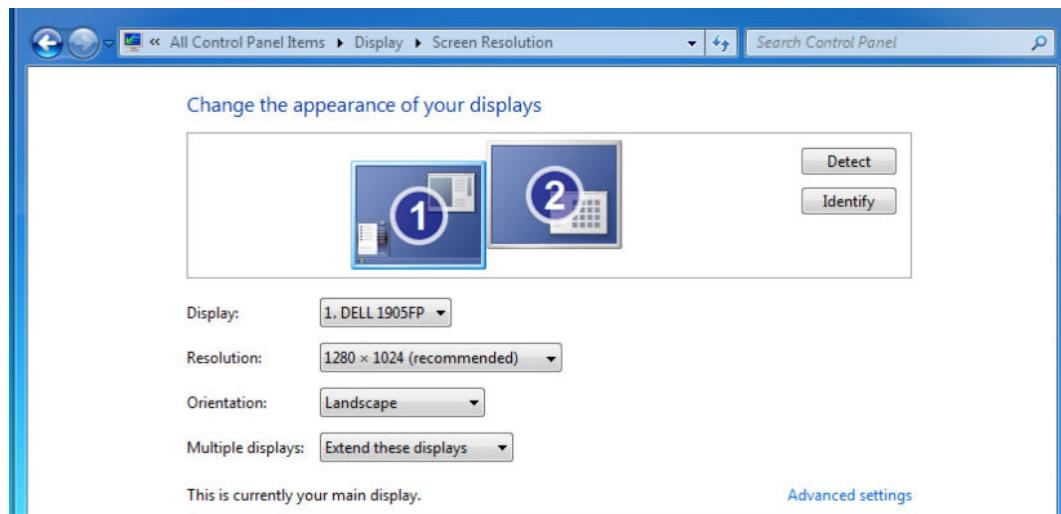
Symptoms

Screen display on one monitor is truncated.

Workaround

Select **Control Panel > Display > Screen Resolution**

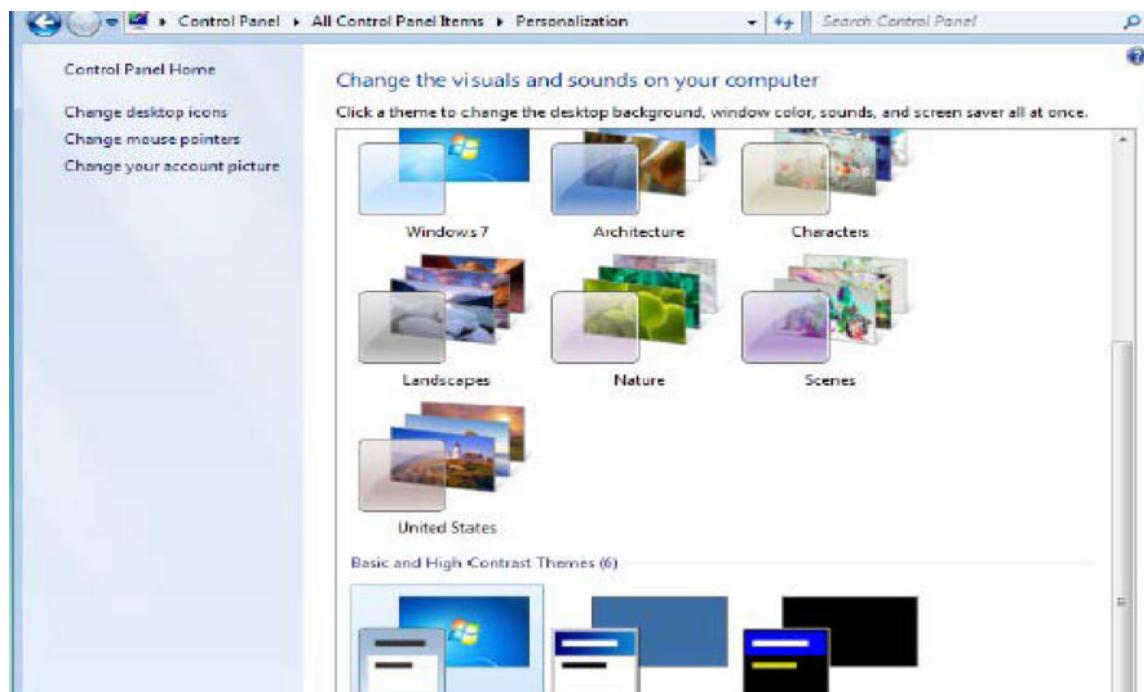
Move the icon for the screen that is truncated, so that it is a little lower than the other icon, then click **Apply**.



3.4.4.6 Client Windows Flicker

Flickering windows in the client browser may indicate that incompatible Windows graphic settings are applied. **Aero themes** are known to cause this problem.

Select **Control Panel > Personalization** and select the **Windows 7 Basic** theme.



3.4.4.7 First Connection to Universal Viewer Client

When launching Internet Explorer to access the Universal Viewer client the first time, you must run IE as Administrator.

Otherwise, some components may not be correctly installed. In this case you will need to uninstall then reinstall the Universal Viewer client, then run launch it for the first time as explained above.

3.4.4.8 Poor Performance on Large Screen Systems

When multiple users are connected to an AW Server, and some are using large-resolution screens, performance may be very slow.

To remedy this, on the workstation(s) with large resolution screens, use Windows **Control Panel > Display > Screen Resolution** to reduce the displayed resolution on the screens used to display AW 3D Applications.

3.4.4.9 AW Server not responding

If AW Server stops responding, on a workstation where you are confident that the integration is correctly configured, and the client and applications have been previously successfully used, you may need to manually kill AW Server client processes on the client PC :

- Launch Windows Task Manager (press Ctrl + Alt + Del then select Start Task Manager)
- Kill the following processes with hierarchy: solomini, nxproxy, xwinGE

3.4.4.10 Poor Performance After Extended Use

After using AW Server in Seamless Integration with Universal Viewer for an extended period, performance may be degraded. In this case, even if all processes are killed, performance will remain slow. In this case, reboot the server (with caution and after customer consultation / warning users via Broadcast Message. Ideally perform reboots outside of core user hours).

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

3.4.4.11 Empty list in Universal Viewer Client

Click on the Search icon to locate missing entries.

3.4.4.12 New images

To retrieve new images in the Universal Viewer Client, click Refresh, or exit 3D Applications.

3.4.4.13 Licensing New Applications on AW Server

The new applications will not be reflected in the 3D Applications list in Universal Viewer until the Tomcat service has been restarted on the Universal Viewer using Integrat Control Panel (do this with extreme caution after customer agreement).

3.4.4.14 Seamless cluster configuration support with 40k slices per node

For version prior to AW Server 3.2 Ext. 4.4 the cluster configuration handles 16k slices per node. From AW Server 3.2 Ext. 4.4 the cluster configuration handles 40k slices per node. As there is a need to handle 40k slices per node on each AW Server 3.2 version, the configuration should be updated for version prior to AW Server 3.2 Ext. 4.4:

1. Open the AW Server Console/terminal, login as **root**.
2. Navigate to the `/var/lib/ServiceTools_AWS/conf` directory:
`cd /var/lib/ServiceTools_AWS/conf <Enter>`
3. Backup the `PACSAvailability.xml` file:
`cp PACSAvailability.xml PACSAvailability.xml.orig <Enter>`
4. Using "**vi**" editor open the `PACSAvailability.xml` file:
`vi PACSAvailability.xml <Enter>`

5. Using the **<arrow>** keys, go to the xml block starting with:

```
<hardwareType type="virt" tier="low">
```

6. Move the cursor till the last line of this block, just before:

```
</hardwareType>
```

7. Press the **<o>** key to insert a line below the cursor.

8. Copy/paste the following two lines:

```
<config license="SdC_Low_Tier_Premium" isCluster="no"
integMode="seamless_integ" minRequiredMemory="64 GB" />
```

```
<config license="SdC_Low_Tier_Premium" isCluster="yes"
integMode="seamless_integ" minRequiredMemory="64 GB" />
```

9. If needed press **<Backspace>** to remove the empty line inserted.

10. Press **<Esc>** to exit the editor mode.

11. To save the file and exit type **:wq** then press **<Enter>**.

12. Verify that the PACSAvailability.xml file is updated correctly:

```
diff PACSAvailability.xml PACSAvailability.xml.orig <Enter>
```

The two lines added above are displayed in the output of the command.

13. Restart the tomcat service.

```
systemctl restart tomcat <Enter>
```

3.4.5 Tools and tips

3.4.5.1 How to Deal with Intermittent Reboot Hangs on Physical Servers

PROBLEM DESCRIPTION:

Intermittently the server can hang while rebooting. The server will shutdown, and then just hang at a blank console screen, and never begin to report its boot up testing & scripting. Normally, this can take 5 minutes or more at times at a blank screen. If the boot up does not begin after 5 or 10 minutes tops - the following steps should be taken:

SOLUTION(s):

- Can be done remotely by an online engineer, but there will need to be onsite verification of reboot status if the remote tools do not come ready:

If the server's service processor "iLO" web interface is accessible, use the remote power control tools to cycle the server's power –See Chapter 7, [7.8 HP Escalation and Communication Flow on page 464](#) for details of the HP iLO Service Processor. This can perform an automatic power off & back on. System should reboot normally.

- Cannot be done remotely:

If the service processor iLO web interface is not accessible, or fails to reboot the server – press and hold the power button on the front left side of the server until the power shuts down. After a minute, press the power button again to turn the server power back on. System should reboot normally.

Alternatively: Detach power cables from the server and DAS (if applicable), wait 30 seconds, re-attach the power cables to DAS if applicable then wait a further 30 seconds, then reattach the power cables to the server and power up.

- If none of these steps reboot the server – there is a hard server failure and the Vendor hardware break/fix process must be engaged to have the Vendor resolve the issue.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

3.4.5.2 PING

PING is an acronym for the words '**P**acket **I**Internet **G**roper'. This utility is supported by Windows® 7.

The PING utility is essentially a system administrator's tool that is used to see if a computer is operating and also to see if network connections are intact. PING uses the Internet Control Message Protocol (ICMP) Echo function. A small packet is sent through the network to a particular IP address. This packet contains 64 bytes - 56 data bytes and 8 bytes of protocol reader information. The computer that sent the packet then waits (or 'listens') for a return packet. If the connections are good and the target computer is up, a good return packet will be received. PING can also tell the user the number of hops that lie between two computers and the amount of time it takes for a packet to make the complete trip. Additionally, an administrator can use PING to test out name resolution. If the packet bounces back when sent to the IP address but not when sent to the name, then the system is having a problem matching the name to the IP address. The time it takes for the packet to get to the target computer and back again is known as the round trip time. If this takes an extended period of time, it is indicative that something may be wrong.

Blocking ICMP packets on a network at an Internet access point is a common network administration security policy. PING can be used to flood a network as well as discover network resources by malicious Internet entities. Blocking PING within an intranet is more rare, but is also a potential reality.

If your particular AW Server intranet has blocked the PING ICMP Echo function, you will not be able to complete ping tests of the CLIENTS. You will need to either:

- Continue with other tests and see if the CLIENT can connect to the AW SERVER – if so, the PING test is irrelevant.
- Contact and work with the network / IT Admin to allow PING or help you establish the network connection via another method to discover the connectivity status.

3.4.5.3 Trace Route

There is another useful tool that can be employed if the ping connection test shows problems, and IF YOUR WINDOWS® VERSION SUPPORTS IT - **tracert** (TRACEROUTE). (This utility is supported by Windows® 7) The **tracert** command is used to trace a network packet being sent and received and the amount of hops required for that packet to get to its destination. The functionality of TRACERT is essentially the same under all versions of Windows®.

Tracert uses the IP TTL field and ICMP error messages to determine the route from one host to another through a network. Care must be taken with tracert as it shows the optimal route, not necessarily the actual route. To be accurate, it is possible to **ping** from a UNIX machine back to the PC using the -R option to record the route taken - but only if the particular network devices support it.

It is not the purpose of this document to completely describe and support the use of tracert, or any other network analysis tool. It is merely to suggest possible actions to discover network functionality within an AW Server set-up and test phase. Additionally, there are other similar tools available in the network analysis community with GUI features and automated functions that can be used for this purpose also...

Here is an EXAMPLE tracert instance for reference:

Figure 3-9 TRACERT EXAMPLES

```
C:\> C:\WINNT\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>Documents and Settings\krisberg>tracert 3.70.205.110
Tracing route to 3.70.205.110 over a maximum of 30 hops
  1  2 ms  <1 ms  <1 ms  3.70.205.110 ←

Trace complete.

C:\>Documents and Settings\krisberg>tracert 3.70.208.106
Tracing route to 3.70.208.106 over a maximum of 30 hops
  1  1 ms  <1 ms  <1 ms  3.70.204.254 ←
  2  4 ms  <1 ms  <1 ms  3.70.208.106 ←

Trace complete.

C:\>Documents and Settings\krisberg>tracert 3.231.48.127
Tracing route to 3.231.48.127 over a maximum of 30 hops
  1  <1 ms  <1 ms  <1 ms  3.70.204.254
  2  <1 ms  <1 ms  <1 ms  medhdq1us.med.ge.com [3.28.28.98] ←
  3  <1 ms  <1 ms  <1 ms  medadm16us-msfc1.med.ge.com [3.28.28.177]
  4  <1 ms  <1 ms  <1 ms  medwan3us.med.ge.com [3.28.31.139]
  5  7 ms   7 ms   7 ms   mededc1us.med.ge.com [3.7.100.141]
  6  9 ms   6 ms   9 ms   mededc3us.med.ge.com [3.231.35.190]
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  ^C

C:\>Documents and Settings\krisberg>tracert 3.231.48.134
Tracing route to 3.231.48.134 over a maximum of 30 hops
  1  <1 ms  <1 ms  <1 ms  3.70.204.254
  2  <1 ms  <1 ms  <1 ms  medhdq2us.med.ge.com [3.28.28.106] ←
  3  <1 ms  <1 ms  <1 ms  medadm16us-msfc2.med.ge.com [3.28.28.189]
  4  <1 ms  <1 ms  <1 ms  medwan3us.med.ge.com [3.28.31.139]
  5  2 ms   2 ms   2 ms   mededc1us.med.ge.com [3.7.100.141]
  6  9 ms   10 ms  10 ms  mededc3us.med.ge.com [3.231.35.190]
  7  2 ms   2 ms   2 ms  3.231.48.134 ←

Trace complete.
```

3.4.5.4 SSH (Secure Shell)

Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two computers. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which sent information, notably passwords, in plaintext, making it possible to intercept. The Encryption SSH uses provides confidentiality and integrity of data over an insecure network, such as the Internet.

The Encryption SSH uses provides confidentiality and integrity of data over an insecure network, such as the Internet. To use SSH, the host computer must either have SSH internal support, or an SSH tool such as "putty" installed and operable. Most Windows® computers do not have SSH support built-in.

By default, SSH is disabled on the AWS server for security reason. The SSH service is running on the AW Server, however the firewall does not allow connection through SSH. Alternative mechanisms for command-line access are the AWS Service Tools (Terminal Tool), the SSH connectivity tool or the Terminal tool in FFA, and the iLO service processor interface (Console Redirect).

SSH is used for remote service by GE HCS managed servers using remote connectivity (InSite/RSvP). **Keep SSH disabled** for these systems, because there are specific exception rules in the firewall allowing SSH access for these systems.

For GE EDS managed servers (not using remote connectivity (InSite/RSvP)), **enable SSH** to allow remote access.

NOTICE

To protect customer network and data security, SSH must always be disabled when not in use for a deliberate and specific service reason.

NOTICE

SSH is enabled by default for Remote Service connection from GEHC Backoffice.

3.4.5.4.1 Enabling SSH

To enable SSH, preferably use the Service Tools interface as described in [2.5.1.2 Using an ssh client instead of Terminal on page 88](#). If you don't have access to the Service Tools, use the following procedure:

1. Connect to the server command line interface from the local server KVM or the iLO Console Redirect.
2. Login as **root**.
3. Type the command:

```
ssh_enabler -enable <Enter>
```

The message Enabling SSH service... appears.

4. Restart the PNF firewall:
 - From AW Server 3.2 Ext. 4.0:

```
systemctl restart pnf <Enter>
```
 - For AW Server 3.2 Ext. 3.4 and previous versions:

```
/etc/init.d/pnf off <Enter>
iptables -F <Enter>
/etc/init.d/pnf on <Enter>
```

3.4.5.4.2 Disabling SSH

To disable SSH, preferably use the Service Tools interface as described in [2.5.1.2 Using an ssh client instead of Terminal on page 88](#). If you don't have access to the Service Tools, use the following procedure:

1. Connect to the server command line interface from the local server KVM or the iLO Console Redirect.
 2. Login as **root**.
 3. Type the command:

```
ssh_enabler -disable <Enter>
```
- The message Disabling SSH service... appears.
4. Restart the PNF firewall:
 - From AW Server 3.2 Ext. 4.0:

```
systemctl restart pnf <Enter>
• For AW Server 3.2 Ext. 3.4 and previous versions:
/etc/init.d/pnf off <Enter>
iptables -F <Enter>
/etc/init.d/pnf on <Enter>
```

3.4.5.5 AW Configuration file (conf)

The AW configuration file contains a listing of the AWS system configuration as well as all Applications installed on the server. You can display it using the **conf** command.

- Open a Terminal (from the Service Tools), and login as **root**.
- To display the **conf** file, type in:

```
conf | more <Enter> OR
conf -long | more <Enter> (also displays information on Ethernet cards settings)
• To save into a text file, then display, type in:
conf > config.txt <Enter> OR conf -long > config.txt <Enter>
more config.txt <Enter>
```

The following example is the first part of the configuration for a HP DL360 Low Tier server AW Server 3.2 Ext. 3.4:

```
Date: Wed Jan 15 17:19:42 CET 2020
=====
SITE IDENTIFICATION
-----
Hospital name : GE Hospital
System ID : HT88
Country Code : HU
Global Order Number : 1234567
S\N : CZ2424K2R8
=====
STATION CONFIGURATION
-----
Internet address : 3.231.145.95
Netmask : 255.255.255.0
Default gateway : 3.213.154.254
hostname : ht88
DICOM Hostname : ht88
DICOM AETitle : ht88
DICOM Port Number : 4006
CPU : Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
Nr of processors : 20
Processor clock : 2.40GHz
Operating System : HELIOS release 6.10LTM1 (Carbon)
OS Version : 6.10LTM1
Uptime : 9 days
Memory Total / Free : 64300 (MB) / 58348 (MB)
OS Disk Space Total/Free : 49 (GB) / 29 (GB)
Image Disk Space Total/Free : 2196 (GB) / 1747 (GB)
Backup Disk Space Total/Free : 3 (GB) / 3 (GB)
Log Disk Space Total/Free : 9 (GB) / 8 (GB)
Network Queue Status : In progress: 0 Pending: 0 Paused :0 Failed: 0
Mount count curr./max (im. p.): 8/25
Next fsck date (im. part.) : Mon May 25 12:06:12 2020
```

```

Certificate expiration date : Tue 01 Mar 2022 11:09:17 AM CET
Clam AV status : Not activated, 0
Machine type : ProLiant DL360 Gen9
DAS serial number : Not applicable
Platform version : aws-3.2-3.4-1945.2-925d2763
Modality OS version : AWS3.2_OS_5.1 [20191031]
UDI : (01)00840682102384(10)AWS3D2E003D2
Medical Device Item Number [REF] : 5719780
Medical Device Production Control [LOT] : AWS3D2E003D2
BIOS version : P89
LicenseID : 123456aa
Platform Enabler : SdC_Server_Eight_Seats
Install mode : server
DICOM AET (printing) : PR_ht88
Service Processor : 3.213.154.99
InSite Checkout ID : AWTEST88
License Key : 1234567890ABCDEF
Preprocessing License : N/A
Integration type : standalone
Cluster mode : false
Registration status : Permanent
Registration key : 123456789aa

```

NOTE

You can also retrieve the configuration using the **Pull from system** button on the HealthPage.

NOTE

In AWS3.2 Ext. 4.8 and Ext. 4.9 Secured for RMF mode will be commercially available. Therefore, next to Clam AV status the configuration file will also contain the McAfee Antivirus Software status which is the Antivirus software used in RMF mode.

Generic mode:

```

Clam AV status : <Activated or Not activated>
McAfee AV status : Not activated

```

RMF mode:

```

Clam AV status : Not activated
McAfee AV status : Activated

```

3.4.5.6 Client Checker Tool - Concept

NOTE

The Client Checker Tool **is not available** from version AW Server 3.2 Ext. 4.2.

This tool evaluates the client PC configuration and performance for AW Server viability. It provides feedback on the quality of the client hardware, and basic information about the client PC.

NOTICE

This tool is designed to evaluate the client configuration and monitor to help determine if the system is sufficient for the needs of the AW Server client application. This check is an initial evaluation of the operating system and hardware specifications. It is not meant to replace normal QA procedures.

NOTICE

The Client Checker requires Java to be installed on the client PC (it is not installed by default).

The Client Checker performs a basic test of the computer – the memory available, the pixel bit depth setting of the display, the resolution of the display, etc.

To launch the Client Checker Tool manually, click the **Launch** button on the Service Tools home page:

The screenshot shows the AW Server Service Tools interface. At the top, there is a navigation bar with a GE logo, a dropdown menu set to "English", and a UDI number: (01)00840682102384(10)AWS3D2E003D4. Below the navigation bar, there are download links for "Client for Windows" (Version 3.2 Ext. 3.4) and "Client for Universal Viewer" (Version 3.2 Ext. 3.4). A "System Requirements" section lists hardware and software requirements. Under "Operating systems", it lists Windows 7 SP1 32bit and 64bit, Windows 8.1 32bit and 64bit, and Windows 10 32bit and 64bit. It also notes that certain GE consoles are supported. Under "Browsers", it lists Internet Explorer 10.x, 11.x, Firefox, and Chrome. A note states that browser security settings should have Javascript enabled. At the bottom of the page, there are links for "Client Checker Tool" (with a red box around the "Launch" button), "Operator Manuals", "AW Server/3D Viewer/2D Viewer/Volume Viewer" (with a red box around the "Open" button), "Configuration", "Service and Administrative Tools" (with a red box around the "Launch" button), and a legal notice about trademarks and disclaimers.

Client Checker Tool Launch

Operator Manuals **AW Server/3D Viewer/2D Viewer/Volume Viewer** Open

Configuration **Service and Administrative Tools** Launch

GE and the GE Monogram are trademarks of General Electric Company.
Windows and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Intel, Core, and Pentium are trademarks of Intel Corporation in the United States and/or other countries.
JavaScript is a trademark or registered trademark of Oracle and/or its affiliates in the United States and other countries.
Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.
Parallels and Parallels Desktop are registered trademarks of Parallels Software International, Inc.

NOTE

Different PC Operating Systems will be characterized in different ways, so all PC characteristics will not list-out exactly the same on different OS's.

NOTICE

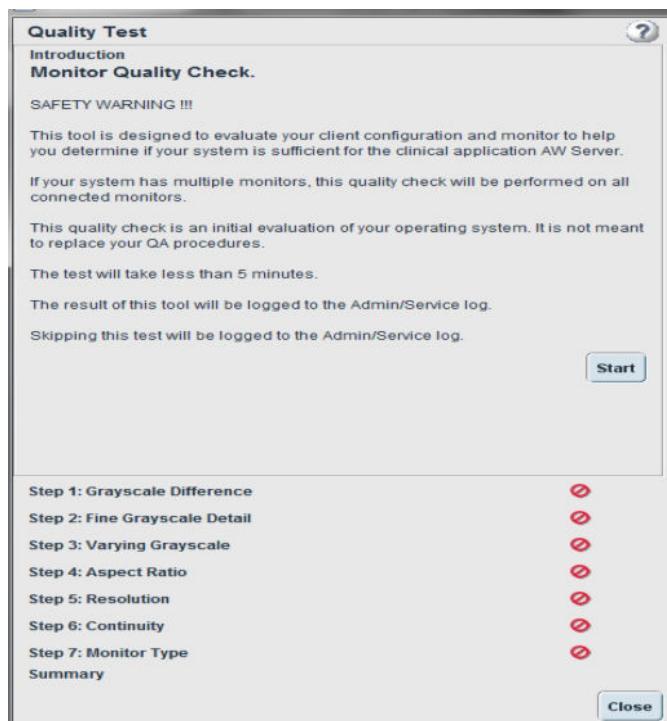
Following this initial check, there will be a prompt to run the monitor quality check routine!!! If the client fails either the initial system compatibility or monitor quality test, it should not be used to support a medical diagnosis. The client may require different settings or a hardware upgrade !!!

3.4.5.6.1 Monitor (Display) Quality Check

The user is directed to run this image quality tool every time there is a change to the monitor, graphic card or monitor cable, or when they dock or undock a laptop, or change viewing conditions – for example, when taking a laptop into or out of a dark reading room.

This evaluation checks the monitor (display). It is based on the user's answers given to visual cues such as how well one can visualize shades of gray, detail, etc. It does not run diagnostic tests on the hardware nor replace normal PC quality assurance checks.

Figure 3-10 MONITOR QUALITY CHECK



NOTICE

THE MONITOR QUALITY CHECK DOES NOT GUARANTEE DIAGNOSTIC QUALITY!

It is only used to determine the basic display functionality of the client. The CUSTOMER is responsible for determining whether client monitors/displays meet all necessary criteria for diagnostic use.

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.

NOTE

When using dual screen, ensure that all monitor is analyzed by the Monitor Quality Check.

3.4.5.6.2 Client Information

The Client information option gathers and displays detailed hardware PC configuration details.

NOTE – the client-checker tool does not do a PORT analysis of the PC. There are no special ports that need to be opened or managed for AW Server. If the PC can access network resources, and download the AW Server Application, it is "network functional" for AW Server purposes.

NOTICE

If the system fails either the initial system compatibility or monitor quality test, the system should not be used to support a medical diagnosis. The system may require different settings or a hardware upgrade.

If the system passes the initial tests it is also important to remember - although the AW Server Client Software can run on PC's meeting minimum specifications - optimal Client performance requires faster PC's. In general, faster CPU speeds result in better interactive performance.

Example results / actions:

- Single core CPU or low CPU speed minimum-spec workstation – suggest that a more powerful machine be used to achieve optimal performance.
- RAM inadequate – suggest adding more RAM.
- Graphics card inadequate – suggest upgrading their graphics card if it does not allow an increase in resolution.
- Monitor quality check failure – suggest to replace the monitor and/or graphics card, and/or monitor cable.
- Basic system test failure – suggest upgrading to a better workstation

3.4.5.6.3 Client Checker Logfiles

Logfiles for data gathered by the Client Checker are stored on the client system in the following locations:

- Linux workstation:
\$HOME/clientchk/ccstatus
- Windows workstation:
%USERPROFILE%/clientchk/ccstatus

NOTE

If these files are required by remote Services, they must be manually retrieved and communicated from the client.

3.4.5.7 Network Performance Measurement Tool (command line tool)

Precondition:

Have an AW Server and a client properly installed.

If you experience performance problems:

If you have a customer complaint about network performance and you have already used the Network tools of the Client and of the Service Tools. performances seem to be due to the customer network.

NOTE

This tool is intended for long time measurements and can saturate the network.

How to use this tool:

This tool uses command lines and is not available through a graphical user interface.

Windows client:

At the client PC, open a Command Prompt window and type in:

- Change dir to *solo* directory:

```
C:\Program Files\GE\AWS_3.2\solo\ <Enter>
```

Alternatively, the path for Windows 64-bit systems is: C:\Program Files (x86)\GE\AWS_3.2\solo\

- Execute (as Administrator) a script that logs in each interval and redirects results to a logfile

```
neta.bat [TYPE] <AW Server_IP_address> [LENGTH ms] [INTERVAL ms] > [logfile] <Enter>
```

Where TYPE is either: download ; upload ; both ; nonblocking ; duplex

Where LENGTH is the measurement duration in milliseconds

Where INTERVAL is the interval between two measures

I.e: short time measurement: download measurement of 10 sec, with interval of 1 sec:

```
neta.bat download 192.10.4.25 10000 1000 > bw1.log <Enter>
```

I.e: long time measurement: download measurement of 3 hours, with interval of 10 sec:

```
neta.bat download 192.10.4.25 10800000 10000 > bw2.log <Enter>
```

- Review the logfile with a text editor or send to AW Engineering for analysis.
- See also the /var/log/gehc/sdc/logfiles/csi_neta.log on the server, which stores bandwidth details for client network communications.

3.4.5.8 Display Performance Measurement Tool (command line tool)

Precondition:

Have an AW Server and a client properly installed.

If you experience performance problems:

If you have a client hardware problem (like too weak video card, or CPU), you could see that the client Native measurement results are low.

How to use this tool:

This tool uses command lines and is not available through a graphical user interface. You will have to setup first the test environment on the AW Server itself, then launch the test from the Client.

During the process you will see 5 different CT image flicker for 13 iterations on Linux, and 14 iterations for Windows. The whole process takes at least 7 minutes to complete.

After the measurement process is done, you will see a "Measurement done, exiting..." line at the end of the console output, any other message would mean that the measurement has not succeeded.

If the measurement was successful, then you can fetch the measurement results from Service Tools' Log Viewer.

3.4.5.8.1 Setup the AW Server for the test

1. Log in to the Service Tools as **service**.
2. In **Tools > Terminal**, open the Terminal tool, login as **root**.
3. Start the server part of the measurement tool by running following command:
`/usr/NX/bin/startdpmtserver.sh <Enter>`.

3.4.5.8.2 Launch the test on the Client

On Windows client environment

Adapt the path to the script in the following examples according to the release version you have installed.

1. Open a Command Prompt window and navigate to the **C:\Program Files (x86)\GE\AWS_3.2\solo\nx** directory:

```
cd "C:\Program Files (x86)\GE\AWS_3.2\solo\nx"
```

2. Start the client part of the measurement tool.

In the Command Prompt type in:

- For unsecure mode

```
startdpmtclient.bat <server's IP address> <Enter>
```

e.g: **startdpmtclient.bat 3.213.160.248 <Enter>**

- For secure mode:

```
startdpmtclient.bat <server's IP address> --secure <Enter>
```

e.g: **startdpmtclient.bat 3.213.160.248 --secure <Enter>**

- To use a proxy server, you have 3 options:

- Manual proxy configuration: for this you need the proxy server's IP address and the port number

```
startdpmtclient.bat <server's IP address> --proxymode manual --proxy <proxyIP:proxyPort><Enter>
```

- User system proxy setting:

```
startdpmtclient.bat <server's IP address> --proxymode system <Enter>
```

- Use automatic proxy configuration

```
startdpmtclient.bat <server's IP address> --proxymode auto --proxy <automatic_proxy_configuration_URL> <Enter>
```

3. Retrieve the results of the test from the AW Server's logfiles

- Log in to the Service Tools as **service**.

- Go to the Log Viewer menu in Diagnostic.

- Filter with the following word "dpmt"

- The log file's format will be: **<client identifier>_<date>_<time>_dpmt.log** and a brief one containing only the measurement results: **<client identifier>_<date>_<time>_briefdpmt.log** (e.g. **c84264ab-c884-4843-a1df-a02dec8a9b02_2014-09-16_17-58-03_briefdpmt.log**).

On Linux client environment:

Not currently supported on AW Server 3.2.

1. Start the client part of the measurement tool.

Standard installation puts AWS client to /usr/share/solo

- For unsecure mode:

```
/usr/share/solo/startdpmtclient.sh <server's IP address> <Enter>
```

i.e.: **/usr/share/solo/startdpmtclient.sh 3.213.160.248 <Enter>**

- For secure mode:

```
/usr/share/solo/startdpmtclient.sh <server's IP address> --secure <Enter>
```

i.e.: `/usr/share/solo/startdpmtclient.sh 3.213.160.248 --secure <Enter>`

- To use proxy server:

```
/usr/share/solo/startdpmtclient.sh <server's IP address> --proxymode
manual --proxy <proxyIP:proxyPort> <Enter>
```

NOTE

On Linux you have only the manual proxy configuration: for this you need the proxy server's IP address and the port number

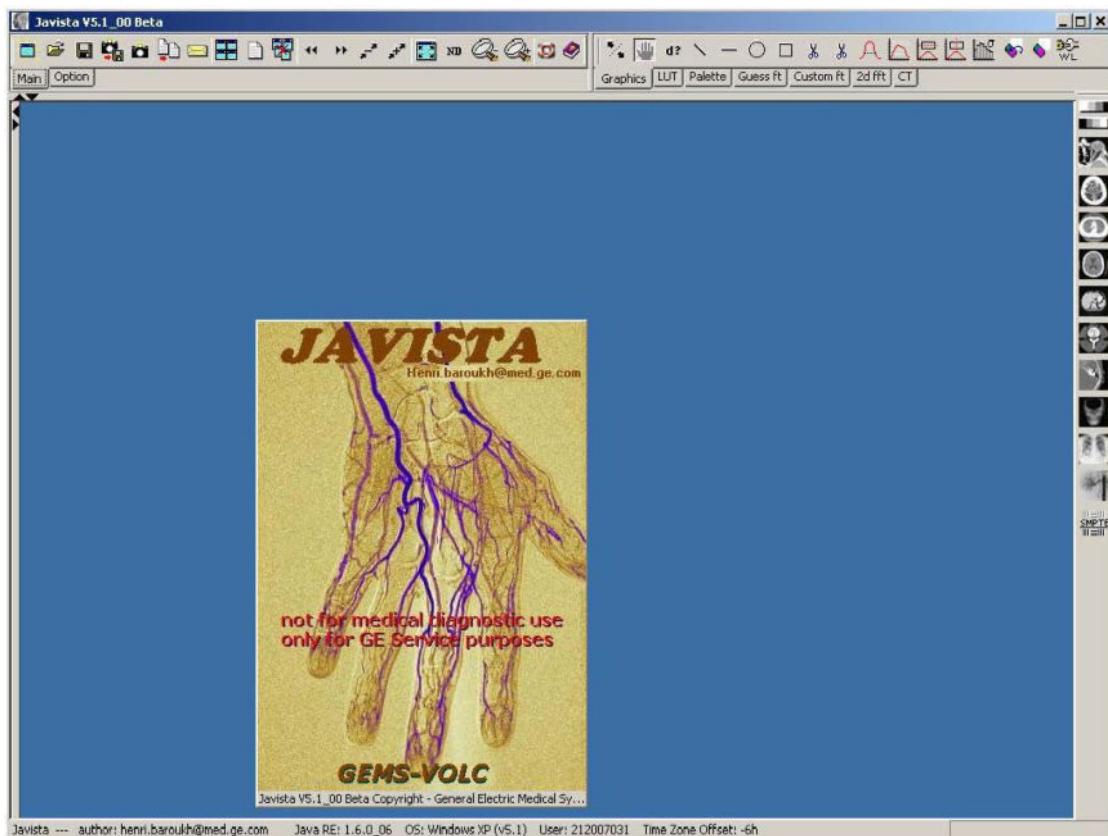
2. Retrieve the results of the test from the AW Server's logfiles

The log file's format will be: `<client identifier>_<date>_<time>_dpmt.log` And a brief one containing only the measurement results: `<client identifier>_<date>_<time>_briefdpmt.log`

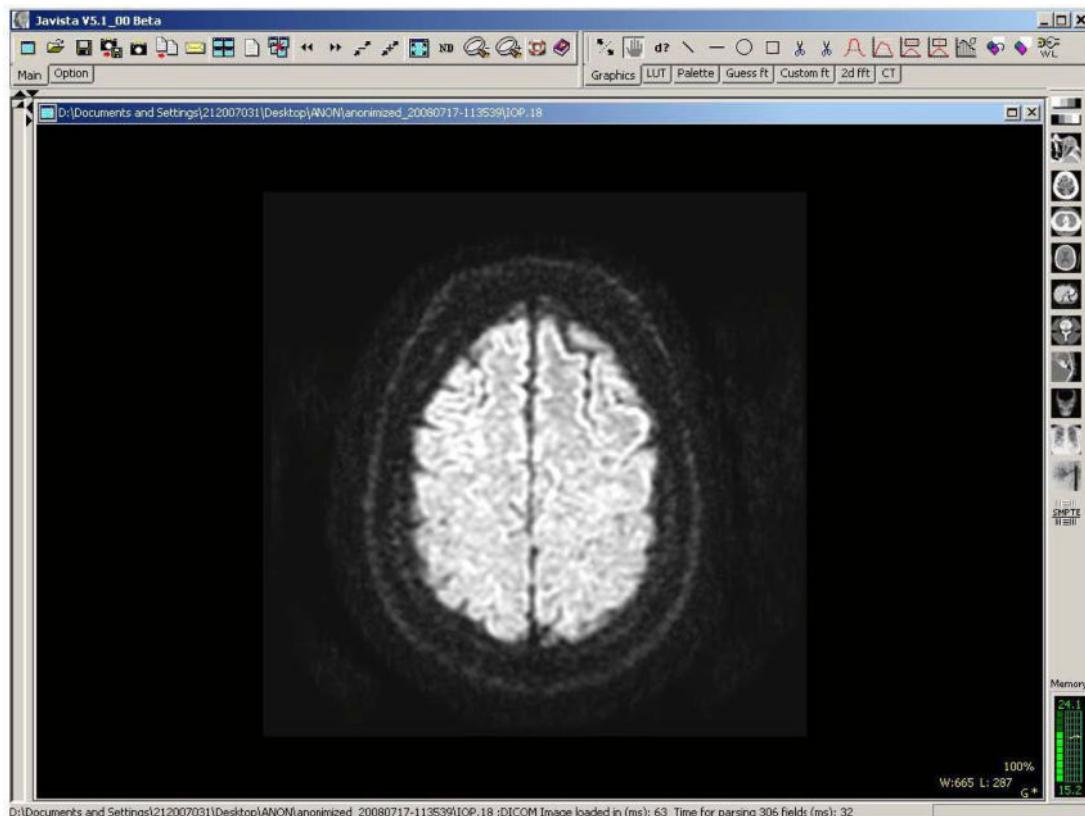
3.4.5.9 Troubleshooting Images

3.4.5.9.1 DICOM Image Viewer

- One of the "**windows**" based DICOM viewer applications (of which there are many available) is the **Javista** application. **Javista** is an application that is currently used by GEHC Service, and is available on the GE Intranet for download and installation. Contact the OLC for details for availability.
- EXAMPLE JAVISTA DICOM VIEWER



- The purpose of this document is not to support the complete capabilities of the *Javista* tool. To display one of the downloaded image files, simply click on the file open ICON, navigate to the file, and click on it. The anonymized image file will display in the tool, and be available for analysis and manipulation.

Figure 3-11 EXAMPLE JAVISTA DICOM VIEWER IMAGE

3.4.5.9.2 Demo Images

NOTICE

Demo images cannot be imported when AWS is configured in Full integration, Seamless or DICOM Direct Connect Integration, because there is no AWS Client Browser. However, demo images can be imported first on the PACS for later usage if the PACS supports this feature.

For the purpose of system testing, demonstration, and training there is one exam/image data loaded during the platform software installation.

This image dataset is embedded in and part of the platform software package. Once removed, the demo images cannot be re-imported directly from the AWS software media.

However, they can be re-imported from the **AWS Demo Exams DVD**, together with more demo exams, from the Client User Interface, using the Tools/Free Image Importer. (**However this is not possible when in Full, Seamless or DICOM Direct Connect Integration mode.**) Refer to the AWS User guide for more precise details.

High level workflow:

- Launch the AWS Client software
- Insert the **AWS Demo Exams DVD** into the corresponding DVD drive
- Click on **Tools** tab
- Click on **Free Image Importer**.
- Click on **Import more images**
- Select **CDROM**
- Search for the compressed diagnostic images file and click **open** to start importing images.

3.4.5.9.3 Removal of Image Data

It is mandatory to use 5534806 - Disk management Tool, when available from your local Pool of Tools and follow instructions given in the 5500610-1EN - Disk Management Tool Service Manual delivered within the kit.

Also refer to Service Note SNAW3037 available on GE Healthcare Documentation Portal, detailing the process for AW's

3.4.5.10 Audit Trail (EAT)

3.4.5.10.1 Overview

This tool is the same interface that appears in the Initial Configuration > Audit trail (EAT). **It is designed and configurable for Enterprise Audit Trail administrative tasks, and also to view the Audit trail log.**

The portion of this tool that has direct use and relevance for AW Server service is the "Viewer" TAB.

This tool and User Interface is taken directly from the EA3 tool-set. The interface has 3 tabs – Local, Repository, and Viewer. The **VIEWER** is where the login authentication history can be viewed. **Make sure that the Audit recording status button is ON.** The **Local** and **Repository** tabs are available for site IT purposes if required.

Audit Trail recording is enabled by default. Leave the settings to the factory default values unless otherwise specified by the IT admin of the site.

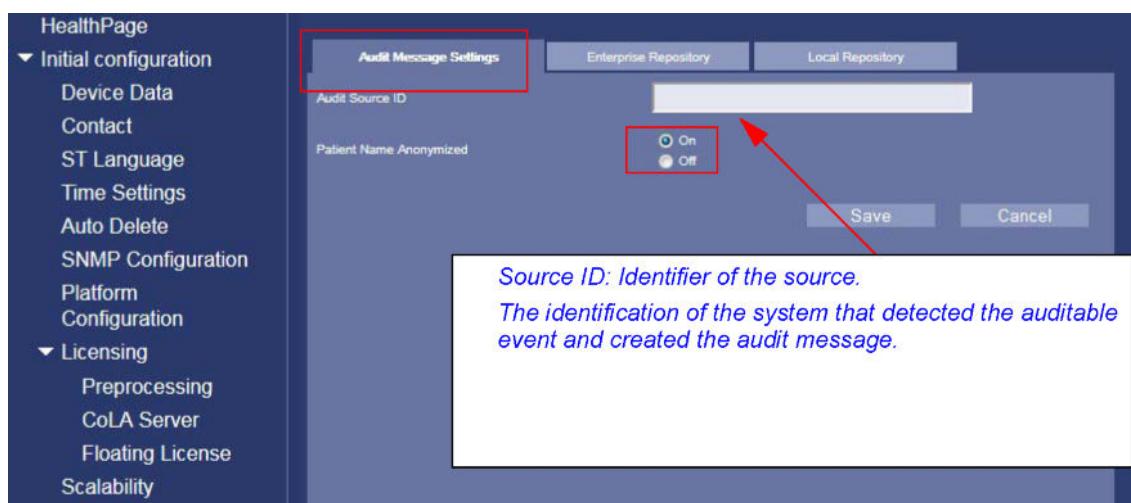
EAT menus are accessible from the **Initial Configuration** menu.

3.4.5.10.2 Audit messages setting

- Click on **Audit Trail (EAT)**. The following menu opens
Note that *Patient Name* is anonymized by default.
- Enter the Audit Source ID.

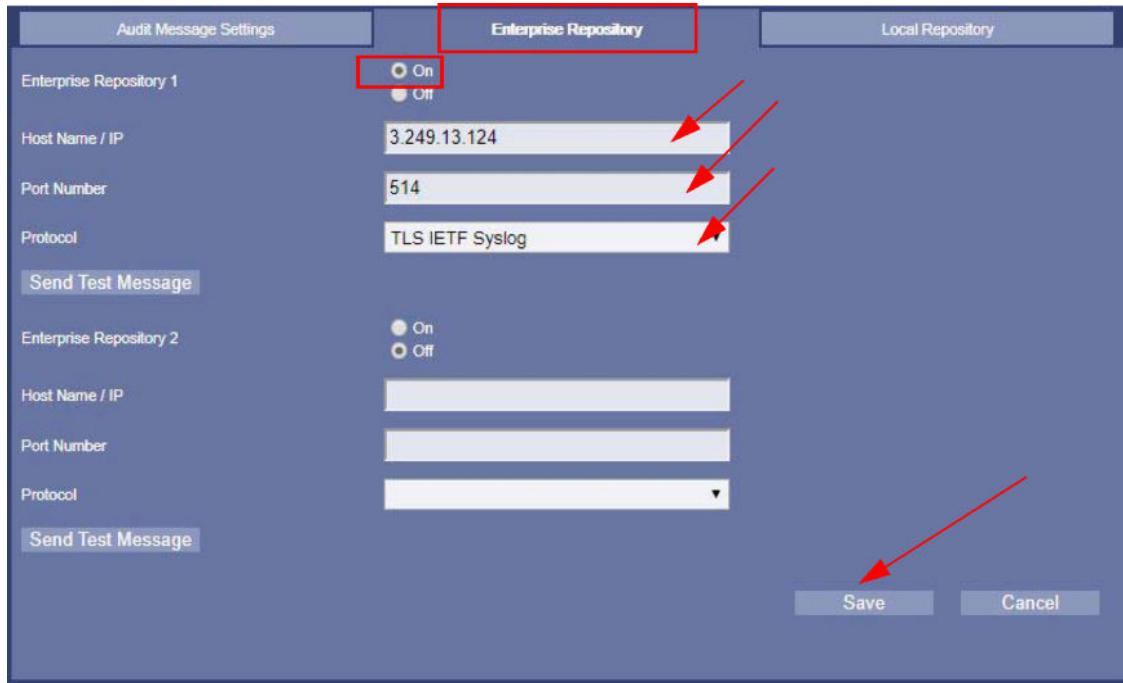
IMPORTANT: The Audit Source ID is mandatory and shall contain either the AW Server Hostname or the Serial Number of the physical AW Server or a value indicated by the site administrator. Then click on **Save**

Figure 3-12 AUDIT MESSAGES SETTING



3.4.5.10.3 Enterprise Repository

If your site is going to use an Enterprise Repository, click on the **Enterprise Repository**. The following screen opens:



Enter the information given by the IT administrator of the site:

NOTE

It is recommended to use an encrypted communication protocol (Transport Layer Security (TSL) protocol) if available, to avoid data to be sent in clear.

1. For a **non-encrypted** communication protocol (e.g.: TCP or UDP protocol):

Enter the Enterprise Repository network information (IP / Port) and select the protocol. Ask the IT admin for the appropriate information.

2. For an **encrypted** communication protocol (e.g.: TLS protocol):

This requires to import the certificate from the site's Enterprise Repository.

Follow the below steps to import the certificate:

NOTE

From AW Server 3.2 Ext. 4.8, this procedure can be done using the Certificate Management page (Refer to the *AW Server 3.2 Installation Manual, Job Card IST010 - Administrative Configuration*), then jump to **Step 2.h**.

- a. Open a Terminal from Service Tools and login as **root**.

- b. Edit the file `/usr/share/gehc_security/eat/configs/tls_config.properties` (using any editor tool) and copy the following lines:

```
tls.keystore=/etc/pki/eat/eatKeyStore.jks
tls.truststore=/etc/pki/eat/eatTrustStore.jks
tls.keystore.password=YXdzMzJfZWFO=
tls.ciphersuite=TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC
_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC
_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC
_SHA256
```

- c. Save and exit the file.

- d. From the prompt, execute the following commands (copy paste all the commands together in the terminal and type <Enter>):

```
chown root:gehc_security /usr/share/gehc_security/eat/configs/ \
tls_config.properties
chmod 0640 /usr/share/gehc_security/eat/configs/tls_config.properties
mkdir -p /etc/pki/eat
chown root:gehc_security /etc/pki/eat
chmod 0750 /etc/pki/eat

openssl pkcs12 -export \
-in /etc/pki/tls/certs/server.crt \
-passin pass:aws32_eat \
-inkey /etc/pki/tls/private/server.key \
-out /tmp/eatCert.pkcs12 \
-passout pass:aws32_eat

rm -f /etc/pki/eat/eatKeyStore.jks
rm -f /etc/pki/eat/eatTrustStore.jks

keytool -v -importkeystore \
-srckeystore /tmp/eatCert.pkcs12 \
-srcstoretype PKCS12 \
-srcstorepass aws32_eat \
-destkeystore /etc/pki/eat/eatKeyStore.jks \
-deststoretype JKS \
-deststorepass aws32_eat
```

- e. Finally execute the following command:

```
keytool -import \
-alias cacert \
-file <EAT_REMOTE_CA> \
-keystore /etc/pki/eat/eatTrustStore.jks \
-storepass aws32_eat <Enter>
```

Where <EAT_REMOTE_CA> is the path of the hospital remote log server's certificate. Check with the site's IT admin or contact the OLC to get it.

A confirmation is required to trust this certificate. Answer yes and type <Enter>.

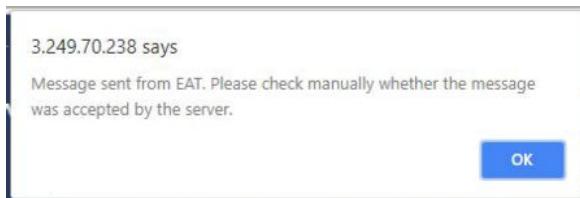
- f. The local host CA (/etc/pki/tls/certs/ca.crt) may need to be copied on the remote log server. Check with the site's IT admin to perform this step if needed.

- g. Edit the file `/usr/share/gehc_security/eat/scripts/EATServer.bat` (using any editor tool) and add the option in the line starting with `java -cp`
- ```
"$GEHC_SECURITY_HOME...:
-DTLS_CONFIG_FILE_PATH=/usr/share/gehc_security/eat/configs/
tls_config.properties
```

So that the line is as follow:

```
java
-cp "$GEHC_SECURITY_HOME/eat/jar/eat.jar":'$GEHC_SECURITY_HOME/eat/
integration/eatsample.jar':'$GEHC_SECURITY_HOME/eat/integration/
eatTest.jar':'$GEHC_SECURITY_HOME/eat/3p/mail.jar'
-DGEHC_SECURITY_HOME="$GEHC_SECURITY_HOME"
-DGEHC_SEC_LANG=$GEHC_SEC_LANG
-Dtterra.eat.model=CLIENT_SERVER -DTLS_CONFIG_FILE_PATH=/usr/
share/gehc_security/eat/configs/tls_config.properties
com.ge.med.terra.eat.server.EATServer $*
```

- h. In the Enterprise Repository tab:
- Enter the Enterprise Repository IP address.
  - Enter the Enterprise Repository port number (by default it is **514**).
  - Select the **TLS IETF Syslog** protocol.
3. Enter information for the second server if applicable.
  4. Click on **Save**.
  5. Reboot the AW Server using the **Reboot AW Server** button from **Tools > Reboot** page.
  6. When reboot in complete, return to **Initial Configuration / Audit Trail (EAT)** page and **Enterprise Repository** tab and click on **Send Test Message**. Check that no error is reported and that the following popup displays:



7. With the IT admin, verify that the remote syslog server (Enterprise Repository) received the test message.
  8. Logout and login from the Service Tools.
- With the IT admin, verify that the remote syslog server (Enterprise Repository) received the test message and the AW Server login message.

### 3.4.5.10.4 Local Repository

If your site **is not going to use** an Enterprise Repository, click on the **Local Repository**. The following menu opens:

The screenshot shows the 'Audit Message Settings' interface. At the top, there are three tabs: 'Audit Message Settings', 'Enterprise Repository', and 'Local Repository'. The 'Local Repository' tab is highlighted with a red box and has a red arrow pointing to the 'On' radio button under the 'Audit Trail' section. Below the tabs, there is a list of audit events with their details. To the right of the list, there are sections for 'Event', 'Active Participant', and another 'Active Participant'.

| Event ID / Time / Event Outcome |                                     |
|---------------------------------|-------------------------------------|
| 110114                          | [2010-02-26T14:24:54] Success       |
| 110114                          | [2010-02-26T14:11:55] Success       |
| 110114                          | [2010-02-26T14:09:55] Success       |
| 110114                          | [2010-02-26T14:02:56] Success       |
| 110114                          | [2010-02-26T14:02:25] Success       |
| 110114                          | [2010-02-26T13:37:41] Success       |
| 110114                          | [2010-02-26T13:35:21] Success       |
| 110114                          | [2010-02-26T13:35:10] Minor Failure |
| 110114                          | [2010-02-26T13:35:08] Minor Failure |
| 110114                          | [2010-02-26T13:15:05] Success       |
| 110114                          | [2010-02-26T13:08:19] Success       |
| 110114                          | [2010-02-26T12:44:36] Success       |
| 110114                          | [2010-02-26T12:44:30] Success       |
| 110114                          | [2010-02-26T12:44:18] Success       |
| 110114                          | [2010-02-26T12:31:45] Success       |
| 110114                          | [2010-02-26T12:31:45] Success       |
| 110114                          | [2010-02-26T12:25:12] Success       |
| 110114                          | [2010-02-26T12:25:12] Success       |
| 110114                          | [2010-02-26T11:54:08] Success       |
| 110114                          | [2010-02-26T11:53:43] Success       |
| 110114                          | [2010-02-26T11:18:46] Success       |
| 110114                          | [2010-02-26T11:15:48] Success       |

**Event**

- Event Date/Time(UTC): 2010-02-26T13:35:21
- Event ID: 110114
- Event Action Code: E
- EventOutcome Indicator: 0 (Success)
- Event Type Code: 110122 (DCM)

**Active Participant**

- User ID: standard@aws1.site
- User Name:
- User Is Requestor: true
- Alternate User ID:
- Network Access Point Type Code: 1 (Machine Name)
- Network Access Point ID: aws1.site
- Role ID Code:

**Active Participant**

Click on the "On" radio button to select Local Repository.

Audit Trail events can be reviewed by clicking on the event to review.

#### NOTE

"UTC" time - conformant with the Audit Trail standard (ANTA)

Notice the file-system location of the log that is used here:

- **/usr/share/gehc\_security/eat/logs/EATLog.x** (Enterprise logs) or
- **/usr/share/gehc\_security/eat/logs/LocalRepository.x** (Local repository logs)

EXAMPLE LOG CONTENTS FOR A SINGLE LOGIN EVENT:

**Jul 25, 2008 12:15:53 PM EAT**

```
ALL: <?xml version="1.0" encoding="UTF-8"?><AuditMessage><EventIdentification EventActionCode="E" EventDateTime="2008-07-25T17:15:53" EventOutcomeIndicator="0"><EventID code="110114" codeSystem-Name="DCM" displayName="User Authentication" /><EventTypeCode code="110122" codeSystem="Log-in" displayName="DCM"/></EventIdentification><ActiveParticipant UserID="212007031" UserName="Lewis Krisberg" AlternativeUserID="" UserIsRequestor="true" NetworkAccessPointID="" /></ActiveParticipant><ActiveParticipant UserID="" UserName="" AlternativeUserID="" UserIsRequestor="false" NetworkAccessPointID="" /></ActiveParticipant><ActiveParticipant UserID="uswaudc03.am.med.ge.com" UserName="Kerberos" AlternativeUserID="" UserIsRequestor="false" NetworkAccessPointID="" /></ActiveParticipant><AuditSourceIdentification AuditEnterpriseSiteID="" AuditSourceID="ct-demo-aws"><AuditSourceTypeCode code="2"></AuditSourceTypeCode></AuditSourceIdentification><ParticipantObjectIdentification ParticipantObjectID="Detail" ParticipantObjectTypeCode="1" ParticipantObjectTypeRole="1"><ParticipantObjectDetail type="Description" value="RUE-zIEF1dGhlbnRpY2F0aW9uIFN1Y2Nlc3NmdWw=" /></ParticipantObjectIdentification></AuditMessage>
```

- Use this **Viewer** log list, and / or the log file itself to evaluate client login history when analyzing client connection issues.
- For instance – if a client cannot connect to the server –
- When was the last time they could?
- What was done to or with their PC since then?
- Are there periodic login failures?
- ... Try to establish some point of reference for determining a possible course of action that might involve the network – or the client configuration that may have changed.

- But, remember – **AT THE END OF THE DAY - THE CLIENT AND THE NETWORK ARE THE RESPONSIBILITY OF THE CUSTOMER...**

**NOTE**

In the viewer, clicking on a line will pop-up the raw data associated with the log entry; clicking outside the box will close the data pop-up.

### 3.4.5.11 Checking Logfiles Collected by Problem Report

The export to backoffice is not activated by default. It must not be activated except by explicit request from Service, IN WHICH CASE YOU WILL BE PROVIDED WITH THE NECESSARY INSTRUCTIONS.

In addition, this functionality is not supported on AW Server installed in EDS environments.

**NOTE**

The Problem Report tool is obsolete since AW Server 3.2 Ext. 4.0.

#### 3.4.5.11.1 Automatic Crash Logging by ProblemReport

The Problem Report feature offers the capability to collect data related to system process errors / application crashes.

Each application has an xml configuration file which lists the resources such as logfiles needed to debug a crash by that application. This tool refers to the Application xml provided by individual applications to get their log file names. It then sends the log file names to the GE back office if InSite is connected. See previous section.

If an Application (new or legacy) crashes, the platform may detect error and invoke the problemReport script which in turn calls reportcollector script.. Problem Report maintains the following logfile:

```
/export/home/sdc/logfiles/problemreporterlog
```

The file contains the following information:

- Name ("Problem Report")
- Problem Report tool's version
- Problem Report Tool's process name and ID
- Timestamp
- Key actions performed
- If InSite is connected, this data is automatically sent to the GE Back Office's global server by the Prodiags task called pd\_aws\_pbreportv2. The report file name contains the workstation model type, system ID and the date.

(This export is transparent to the user and no FE intervention is necessary.)

The destination for the data is: \\(AW backoffice)\\aws\_pbreport.

Data is deleted once it has been sent to the Back Office.

- However if you are called to a site because of an application-related problem, you should try to obtain the Problem Report logfiles from the affected server(s). Check the file location listed above. This needs a configuration of the server to activate the functionality in advance.

**NOTE**

Problem Report also logs details of image exam series from the user's current selection. If any images are subsequently required by GE as part of a crash investigation, make sure you anonymize the images (for instance using the Anonymous Maker utility) before taking/sending this data off-site.

**NOTE**

If Insite is configured on the System, but the GE Back Office cannot be reached, the logfiles remain in the ProblemReport directory for 7 days. Old data is cleaned from the ProblemReport directory every 7 days.

### **3.4.5.11.2 problemReport.sh script**

A script named "problemReport.sh" is provided in the \$SDC\_HOME/scripts directory (for example /export/home/sdc/scripts). Execute this script to capture the following information:

- Platform configuration file
- Output of "ps" command when the script was called.
- Output of "top" command when the script was called.
- Selection file provided by the applications in the XML file using the tag <selection>. As this tag is an "optional" tag, if this information is not provided, capture the default selection file. For any specific reason, if default selection file is not available, selection file won't be copied.
- Logfile names (the "names" of all the log files (in \$SDCHOME/logfiles) that were updated in the one minute period prior to the time the script was called.
- Any other files (Optional) . Applications may request any specific file using the tag <file>.
- XML file provided by applications.
- All the files/sub directories below the directory name specified in the dir element.
- Output of the command(s) mentioned using the XML element command.

The script bundles all the above information into a single file named using the following conventions:

<ProblemReport>\_<sysID\_licID>\_<problem-report-timestamp>.zip

The file is sent to the Back Office (if possible) using ProDiags when configured, assuming the system is connected via InSite and the export to back office is configured - See previous section.

### **3.4.5.12 MEBEF**

MEBEF (Mean Exams Between Exam Failures) data is useful in understanding application usage patterns and their reliability. At installation time, applications register a MEBEF calculation script.

The pd\_aws\_mebef ProDiags task is triggered every Monday at 15:00 to run each of the registered application MEBEF scripts. It creates a consolidated MEBEF report in an XML file and sends it to the GE Back Office (assuming the system is connected via InSite or RSvP).

The MEBEF data is automatically sent to back office with the prodiags task: pd\_aws\_mebef

The Back Office AutoSC location is : \\(AW backoffice\aws\_mebef where (AW backoffice) is a directory available in GE Back Office

### **3.4.5.13 Application Usage Monitor (AUM)**

For more information about AUM, refer to [2.4.2.4 Application Usage Data on page 84](#).

### **3.4.5.14 Antivirus Software on the AW Server**

- On AWS3.2 Ext. 4.8 and prior versions, Generic mode AW Server uses ClamAV®. Refer to the AW Server 3.2 Installation Manual, section ClamAV®.
- On AWS3.2 Ext. 4.8 and Ext. 4.9, Secured for RMF mode AW Server uses McAfee Antivirus Software. Refer to the AW Server 3.2 Installation Manual, section Secured for RMF mode.

## 3.4.5.15 Windows Anti-virus / Security Software on the Client Workstation

### 3.4.5.15.1 Symptoms

Anti-virus or security software installed on the client workstation's host operating system (Windows) may cause problems with the AW Server client and/or Universal Viewer client (depending on integration mode).

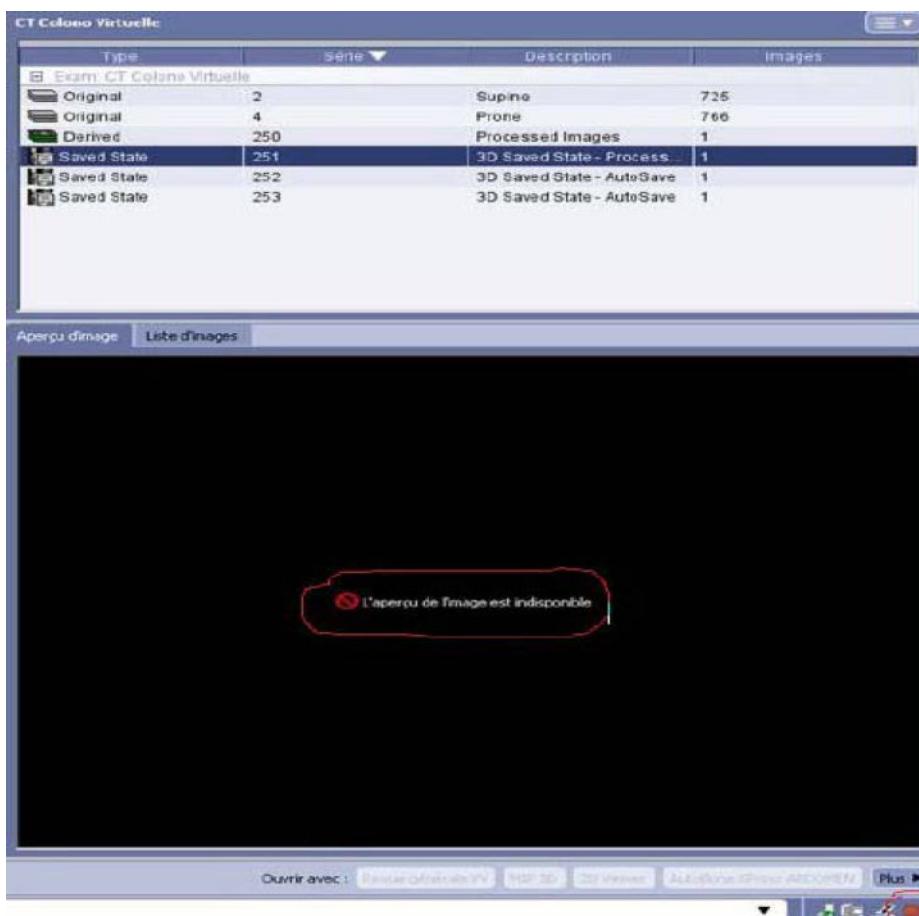
- Some or all of the following symptoms may occur:
- The patient list may display the following error message:

#### *Display Error*

##### *Local display could not be initialized*

- You cannot display an exam series or open any application.
- Under the orange icon it indicates that the remote display is disconnected.
- A red LED appears on the lower right hand corner of the client, and for up to a minute no image is displayed in the Worklist.

An error message may display, for instance indicating that the image preview is unavailable or that there is 'no connection to the DB':



- 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 Client. However, the following are known to cause these problems:

- TrendMicro Antivirus products
- McAfee Antivirus / Security products

**NOTE**

To avoid confusion, please note that it is not about the McAfee Antivirus software running on AW Server, but the one which is installed on the client machines by the Customer.

For the same reason, it is not possible to give a generic workaround. However, take the following into account:

### **3.4.5.15.2 Workaround Strategies**

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 White List / Trusted / Safe Application / Exclusion list:

- solo.exe
- nxproxyGEAWE32.exe

You may need to give full paths to these executables.

If Seamless Integration mode is configured, it is possible that processes related to the Universal Viewer client will also be affected by antivirus software, and must be added to the White List as well.

In the worst case, you may need to manually add the affected processes to a White List via the Windows Registry, as in the following example.

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.

**NOTE**

Always consult with customer IT Admin before making changes to workstation configurations, especially if these affect security.

**NOTICE**

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

### **3.4.5.15.3 Example Workaround for TrendMicro Antivirus**

The following example explains how to add the AW Server client processes to the White List.

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"="nxproxyGEAWE32.exe"
```

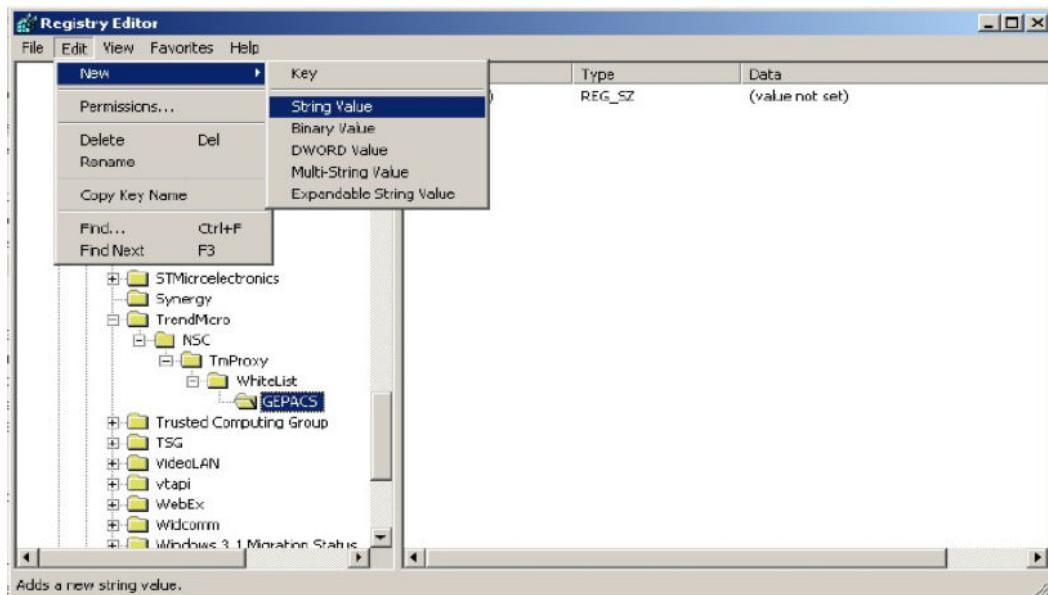
**Procedure:**

Click Start, click Run, type regedit in the Open box, and then click OK.

Navigate to or create the key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\NSC\TmProxy\WhiteList\

Right-click the WhiteList key folder and select New > key...String value

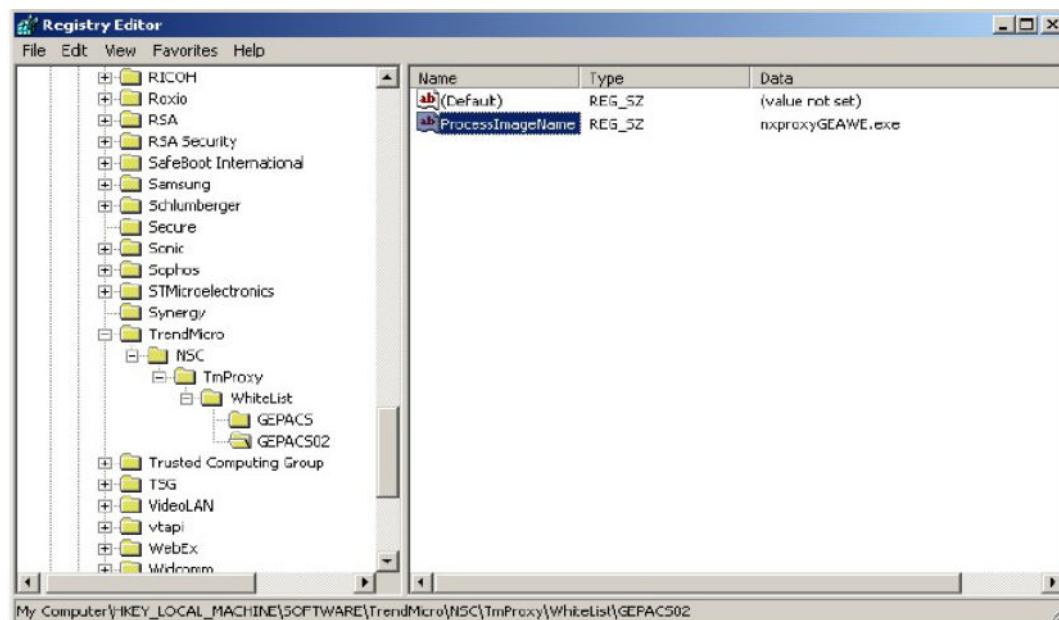


Click on the new key then right click on the right window panel select new string value name it "ProcessImageName".

Right click the ProcessImageName and select Modify, then enter the process name (nxproxyGEAWE32.exe) in the Value data field. Click OK

Repeat the above procedure for the GEPACS02 \ solo.exe key.

Your WhiteList should now contain the new GEPACS and GEPACS02 keys:



Now close the Registry Editor.

It is strongly recommended to reboot the workstation after making changes to the Registry.

### NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

## 3.4.5.16 Server Firewall (PNF)

### 3.4.5.16.1 Overview

The AW Server PNF (**Product Network Filters**) software and configuration is automatically installed with the platform software load. It is automatically enabled and configured in a "default" configuration for the AW Server environment, and should not require any service intervention.

For this reason, there is no PNF interface in the Service Tools web interface. If, exceptionally, changes are needed to the PNF configuration, this can be done via the Linux command line.

The following is for "information" only. Under "normal" circumstances, the PNF configuration should need to be altered by field service.

The PNF has two modes of operation: **ON** and **OFF**.

- In the **ON** state/mode, PNF will allow only the network communications that are specified by its configuration and reject all the rest.
- In the **OFF** mode, PNF will allow all communication (subject to only the filters set by the modality script).

#### NOTICE

If the PNF Firewall is turned off, and left off, this will introduce the server to a security risk. Malicious users can login via SSH and access, corrupt, or delete sensitive files. The server can be used for unauthorized purposes. Vulnerability scans will fail... etc...

The mode can be changed using the PNF manager CLI, and is persistent across reboots.

Configuration of the firewall (**iptables**) in PNF is performed in three stages: **modality script**, **applied filters**, and **modality filters**. Each of these stages can install a set of rules into the iptables filtering software, through which all incoming network packets are sent. Initially, and each time "Factory Settings" is invoked via the CLI command, the dynamic and applied filters files are populated from the default filters file **default.filters**.

The dynamic configuration of PNF often needs to be saved and restored on a product system. The files that need to be saved in this case are: **dynamic.filters**, **backup.filters** and **pnf.run**. Therefore a save and restore operation must record the state of this file (whether it exists or not) in order to preserve the last on/off mode after a restore.

**Usage (CLI)** - The /usr/share/pnf/manager command-line utility is the main entry point into the operation of PNF. It is responsible for applying the filtering rules of PNF and managing its operational mode. The GUI tools invoke it for these operations. Its usage is described below. A brief usage text is printed if manager is invoked without any parameters.

**/usr/share/gehc\_security/pnf/manager <action> <Enter>**

Where **<action>** is one of:

- **restart** - restarts firewall with the current rules (normally, this will have no effect!)
- **on | off** - change the operational mode to ON or OFF (persists at next reboot)
- **status** - print the current operational mode (ON/OFF) to standard out
- **listipt** - lists IPv4 rules currently in effect
  - **listipt6** - lists IPv6 rules currently in effect
- **version** - returns GEHC CSE-P version of PNF

### 3.4.5.16.2 Default PNF settings

- For InSite connectivity (version prior to AW Server 3.2 Ext. 4.2), the 3 IP addresses are defined in the firewall, rule SSH is also enabled for these IP addresses.
- If DNAT IP is setup in remote Service Tools, it will also be enabled for SSH.
- SNMP port is opened on AWS to accept connection from the Service processor IP.

In the below section, there are some information points about the AW Server PNF implementation. Also, a screenshot example that displays the **manager listipt** command output, and the **iptables -L** command output. There must be **root** permissions to run those commands.

The "Source" IP Addresses are filter entries to allow remote connectivity. Connections can be established on the following networks:

- Standard (150.2.0.0/16)
- UK N3 net (10.190.64.0/24)
- Sweden SJUnet (82.136.152.0/24)

#### NOTE

Some network filters/scanners may incorrectly report connection between GE system and GE back-office as suspect.

When the system is remotely connected (InSite or RSvP), connections are regularly established with the GE back-office.

All data exchanged with the GE back-office are considered as normal and shall not be considered as suspect.

PNF currently allows SSH for the above IP Addresses.

Port **22** is shown as allowed in the example, but in the production version, it will **NOT** be allowed from any outside IP Address Source - Secure Shell (SSH).

### 3.4.5.16.3 Command line AWS normal filter

- "Modality filters" is presented under the **/usr/share/gehc\_security/pnf/filters** directory.

**Figure 3-13 PNF EXAMPLE CONFIGURATION OUTPUT**

```
[root@awservc14 ~]# /usr/share/gehc_security/pnf/manager listipt
Chain PNF_DYN (1 references)
pkts bytes target prot opt in out source destination
 5 260 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
 0 0 ACCEPT tcp -- * * 150.2.0.0/16 0.0.0.0/0 tcp dpt:22
 0 0 ACCEPT tcp -- * * 62.130.238.0/24 0.0.0.0/0 tcp dpt:22
 0 0 ACCEPT tcp -- * * 82.136.152.0/24 0.0.0.0/0 tcp dpt:22
 0 0 ACCEPT tcp -- * * 10.190.64.0/24 0.0.0.0/0 tcp dpt:22
 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:4006
 66 3432 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 0
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 3
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 4
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8 l;
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 11
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 12
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 14
 0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 16
 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:17777
 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:17767

[root@awservc14 ~]# /sbin/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT all -f anywhere anywhere
BAD_FLAGS tcp -- anywhere anywhere
SYN-FLOOD tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,ACK/SYN
DROP all -- 255.255.255.255 anywhere
PNF_DYN all -- anywhere anywhere
DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain PNF_DYN (1 references)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- 150.2.0.0/16 anywhere tcp dpt:ssh
ACCEPT tcp -- 62.130.238.0/24 anywhere tcp dpt:ssh
ACCEPT tcp -- 82.136.152.0/24 anywhere tcp dpt:ssh
ACCEPT tcp -- 10.190.64.0/24 anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:pxc-spvr
ACCEPT tcp -- anywhere anywhere tcp dpt:http
ACCEPT tcp -- anywhere anywhere tcp dpt:https
ACCEPT icmp -- anywhere anywhere icmp echo-reply
ACCEPT icmp -- anywhere anywhere icmp destination-unreachable
ACCEPT icmp -- anywhere anywhere icmp source-quench
ACCEPT icmp -- anywhere anywhere icmp echo-request limit: avg 2/sec burst 5
ACCEPT icmp -- anywhere anywhere icmp time-exceeded
ACCEPT icmp -- anywhere anywhere icmp parameter-problem
ACCEPT icmp -- anywhere anywhere icmp timestamp-reply
ACCEPT icmp -- anywhere anywhere icmp type 16
ACCEPT tcp -- anywhere anywhere tcp dpt:sw-orion
ACCEPT tcp -- anywhere anywhere tcp dpt:17767
```

ssh Addresses

Port numbers

Service names

### 3.4.5.17 "awsmonitor" Script

AWS system main parameters and daemon processes are monitored by the `awsmonitor.sh` script that is available at the `/usr/share/ServiceTools_AWS/scripts/monitoring/awsmonitor.sh` file. The script is automatically started at system boot time by the `awsmonitor` `init.d` script (`/etc/init.d/awsmonitor`).

1. What the `awsmonitor` script does:

The `awsmonitor` script monitors / records the following parameters every 30 seconds:

- Date both in human readable form and in UNIX time

- Number of logged in users
- This equals number of nxagent processes running / 4
- Number of AWS applications running
- Voxtool
- GSI Viewer
- SmartScore
- AdvSim
- Adv4D
- Process information
- Number of all processes
- Number of zombie processes
- Disk status for partitions mounted on /, /export/home1, /export/backup
- Mount point
- Total Size
- Used size
- Available size
- Use in %
- System memory status
- Total memory available
- Free memory available
- Used swap size
- awsmonitor shall record system CPU usage
- User space CPU usage
- System CPU usage
- Idle %
- Wait %
- St %
- CPU load for 1, 5, 15 mins
- awsmonitor script also monitors the main AWS daemon processes for PID, %CPU, Resident Set Size, Virtual Memory Size, Number of threads, start\_time, number of file descriptors and pipes
- awsmonitor supports logging these parameters for individual processes
- awsmonitor supports logging these parameters for programs that use fork to create child processes. Examples are Apache2 (httpd1-prefork processes) and PostgreSQL (postmaster processes). In this case the accumulated values are logged for these processes.

## 2. Logging

AWS monitor logs to the `/var/log/gehc/awsmonitor.log` file.

- This logfile is logrotated according to the `/etc/logrotate.d/awsmonitor` configuration file.
- It logrotates the file on a daily basis if the file size is over 44 MB (~ one week logfile).

- The compressed files includes the date of creation in their names.
- Logrotated files that are older than 365 days are deleted and maximum 99 logrotated compressed files are created.
- The awsmonitor script is logrotated in order to be able to continue logging after logrotate.

### 3. Processing the logfile

LogFile can be analyzed just simply by reading it, or by processing it with data visualizer applications like *gnuplot*. In order to help parsing the logfile, each section of a *logrecord* starts with column that name the section. It also includes a number that describes which column is this column.

An example of such section is:

[Memory-348] Total: 65836852 Free: 58241836 Swap: 0

Section name = Memory – this section provides information regarding system memory

348 = This is the 348th column in this log record. It is easy to calculate from this number that total memory is stored in the 350th column while free memory is in the 352nd column and swap size is the 354th column.

### 4. Nice value

"awsmonitor" runs with nice level +10, in order to avoid impact on other processes.

### 5. Switching off and on the awsmonitor script.

The awsmonitor script is automatically started at system boot time, so nothing needs to be done. However, if needed, it can be switched off through the standard tool.

Open a Terminal and type in:

**chkconfig --del awsmonitor <Enter>**

To enable the script again:

**chkconfig --add awsmonitor <Enter>**

## 3.4.6 AW Server workarounds

| Applicability*                                                                           | AW Server 3.2 Extension |     |     |     |     |     |     |     |     |     |     |     |
|------------------------------------------------------------------------------------------|-------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|                                                                                          | 1.0                     | 1.2 | 2.0 | 3.0 | 3.2 | 3.4 | 4.0 | 4.2 | 4.4 | 4.6 | 4.8 | 4.9 |
| 3.4.6.1 Service Tools window does not resize when Browser window is resized on page 215  | X                       | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   |
| 3.4.6.2 Service Tools menu/tab does not display on Firefox on page 216                   | X                       | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   |
| 3.4.6.3 High Tier Load Failure on page 217                                               | X                       | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   |
| 3.4.6.4 Backup/Restore compatibility issue with DI-COM hosts on page 217                 |                         |     | X   | X   | X   |     |     |     |     |     |     |     |
| 3.4.6.5 Logfile partition full on page 218                                               |                         |     | X   |     |     |     |     |     |     |     |     |     |
| 3.4.6.6 AW Server Client login fails due to DLL mistake on page 219                      | X                       | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   | X   |
| 3.4.6.7 Users disconnected following an unexpected CoLA License Server crash on page 219 |                         |     |     | X   |     |     |     |     |     |     |     |     |
| 3.4.6.8 Remote node control enabled on page 222                                          |                         |     |     |     | X   | X   |     |     |     |     |     |     |
| 3.4.6.9 Unexpected network traffic sent from AW Server on page 223                       |                         |     |     |     | X   | X   |     |     |     |     |     |     |

| <b>Applicability*</b>                                                                                                     | <b>AW Server 3.2 Extension</b> |            |            |            |            |            |            |            |            |            |            |            |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| <b>Problem (headline)</b>                                                                                                 | <b>1.0</b>                     | <b>1.2</b> | <b>2.0</b> | <b>3.0</b> | <b>3.2</b> | <b>3.4</b> | <b>4.0</b> | <b>4.2</b> | <b>4.4</b> | <b>4.6</b> | <b>4.8</b> | <b>4.9</b> |
| 3.4.6.10 Incoming DICOM transfer attempts fail on page 223                                                                |                                |            |            |            | X          |            |            |            |            |            |            |            |
| 3.4.6.11 Cannot save Postscript printer when the IP address contains a 0 on page 226                                      |                                |            |            |            | X          |            |            |            |            |            |            |            |
| 3.4.6.12 Hard drives check command not working on HPE ProLiant DL360 Gen9 Server on page 227                              |                                |            | X          | X          | X          | X          |            |            |            |            |            |            |
| 3.4.6.13 DICOM requests (C-FIND) character representation not supported by older systems on page 228                      | X                              | X          | X          | X          | X          | X          | X          | X          | X          | X          | X          | X          |
| 3.4.6.14 AW Server Client login fail due to display error on page 228                                                     | X                              | X          | X          | X          | X          |            |            |            |            |            |            |            |
| 3.4.6.15 EA3 authentication using SSL connection with Active Directory not working on page 228                            |                                |            |            |            |            | X          | X          | X          | X          | X          | X          | X          |
| 3.4.6.16 AW Server Client connection with the AW Server is lost on page 229                                               | X                              | X          | X          | X          | X          | X          |            |            |            |            |            |            |
| 3.4.6.17 Updating the AE Title following the host-name characters policy change in OS 6.0 (HeliOS 7.7) on page 230        |                                |            |            |            |            |            | X          | X          | X          | X          | X          | X          |
| 3.4.6.18 CoLA server not running after software update or system reboot on page 230                                       |                                |            |            |            |            | X          |            |            |            |            |            |            |
| 3.4.6.19 Restore fails if the built-in Floating License server (CoLA) is disabled on page 232                             |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.20 Norwegian language support for Solo Client on AW Server Seamless integration mode on page 233                    |                                |            |            |            |            | X          |            |            |            |            |            |            |
| 3.4.6.21 DICOM Direct Connect performance issues on page 233                                                              |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.22 Cluster certificate application issue on page 234                                                                |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.23 AW Server Client applications cannot start due to inappropriate user rights on Windows on page 235               |                                |            |            |            | X          | X          | X          |            |            |            |            |            |
| 3.4.6.24 Outgoing DICOM communication failure (C-FIND, C-STORE) on page 236                                               |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.25 Licenses for applications not installing after an AW Server update or upgrade on page 238                        |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.26 Backup/Restore compatibility issue with AW Server AET port number on page 239                                    |                                |            |            |            |            |            | X          |            |            |            |            |            |
| 3.4.6.27 DICOM transfer failure when DICOM Host Access Control change without system restart on page 240                  |                                |            |            |            |            |            | X          | X          | X          | X          | X          | X          |
| 3.4.6.28 Cannot install the Edison Machine Light and Service outside the GE network on page 240                           |                                |            |            |            |            |            |            | X          |            |            |            |            |
| 3.4.6.29 Service/admin user login problems and/or log partition getting full causes system to get unavailable on page 241 |                                |            |            |            |            |            |            | X          | X          |            |            |            |
| 3.4.6.30 AW Server on CT Nano-Cloud does not start after CT Console reboot on page 246                                    |                                |            |            |            |            | X          | X          |            |            |            |            |            |

| <b>Applicability*</b>                                                                                                                                | <b>AW Server 3.2 Extension</b> |            |            |            |            |            |            |            |            |            |            |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
|                                                                                                                                                      | <b>1.0</b>                     | <b>1.2</b> | <b>2.0</b> | <b>3.0</b> | <b>3.2</b> | <b>3.4</b> | <b>4.0</b> | <b>4.2</b> | <b>4.4</b> | <b>4.6</b> | <b>4.8</b> | <b>4.9</b> |
| <a href="#">3.4.6.31 Service restart and data loading problems on page 246</a>                                                                       |                                |            |            |            |            |            |            |            |            | X          |            |            |
| <a href="#">3.4.6.32 Application Usage Monitor not working in NanoCloud AW Server on page 248</a>                                                    |                                |            |            |            | X          | X          |            |            |            |            |            |            |
| <a href="#">3.4.6.33 Cannot mount USB media on Nano-Cloud on page 249</a>                                                                            |                                |            |            |            |            |            | X          | X          | X          | X          | X          | X          |
| <a href="#">3.4.6.34 Database corruption in Nano-Cloud AW Server on page 250</a>                                                                     |                                |            |            |            | X          | X          |            |            |            |            |            |            |
| <a href="#">3.4.6.35 Filmer export to PDF function does not work on page 250</a>                                                                     |                                |            |            |            |            |            | X          | X          | X          | X          | X          | X          |
| <a href="#">3.4.6.36 EA3 component corruption after system configuration restoration failure on page 250</a>                                         |                                |            |            |            |            |            |            | X          | X          | X          | X          | X          |
| <a href="#">3.4.6.37 Platform analytics sweep scripts cannot get application usage information from sites on page 253</a>                            |                                |            |            |            |            |            |            | X          | X          | X          |            |            |
| <a href="#">3.4.6.38 Login panel is not displayed in Certificate Management page on page 254</a>                                                     |                                |            |            |            |            |            |            | X          | X          | X          |            |            |
| <a href="#">3.4.6.39 3D application not starting after restoring backup containing Web Client settings on page 256</a>                               |                                |            |            |            |            |            |            | X          | X          | X          | X          |            |
| <a href="#">3.4.6.40 Cannot load Save State created by AW Server applications in Micro Cloud (AW Server hosted by Edison HealthLink) on page 256</a> |                                |            |            |            |            |            |            |            |            |            | X          |            |
| <a href="#">3.4.6.41 Cannot open 2D datasets on AW Enterprise systems on page 257</a>                                                                |                                |            |            |            |            |            |            |            |            |            | X          | X          |

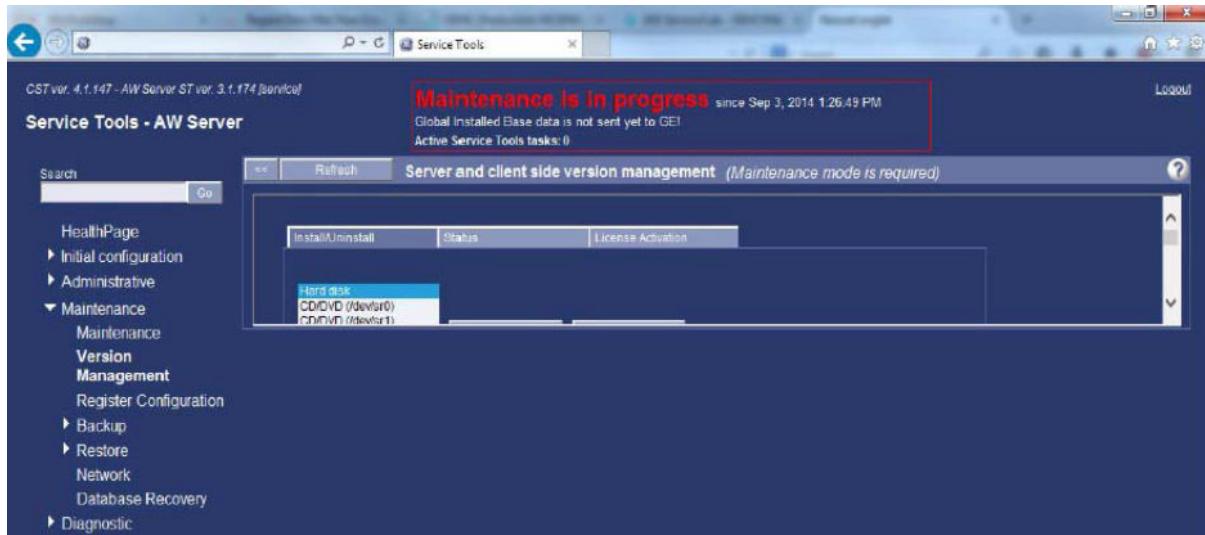
\*An empty cell means the problem is not present or has been fixed in the corresponding extension.

#### NOTE

In the below workarounds when a file is updated, it is requested to backup it (copy the file into <filename>.orig – the extension may differ). So, if some mistakes occur while executing the workarounds, it is recommended to recover the backup file (copy the backup file into the original file) and to re-execute the workaround.

## 3.4.6.1 Service Tools window does not resize when Browser window is resized

**Issue:** The Service Tools window does not occupy the whole space of your Browser window, as shown below:



**Cause:** this issue happens when

1. You resize your Internet Browser window to be small.
2. You open a Service Tools menu.
3. You resize your Internet Browser window to occupy the whole screen.

The Service Tools menu is keeping the window size that was set when it first opened.

**Solution:** Maximize your window to ensure that it occupies the whole screen. Then hit the refresh button at the top of the Service Tools, below the Service Tools header.

### 3.4.6.2 Service Tools menu/tab does not display on Firefox

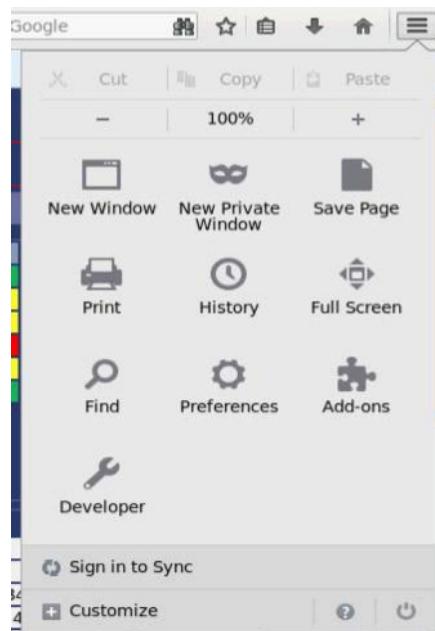
**Problem:** When navigating in the Service Tools with Firefox (locally on the AWS), some menu/tab do not open after clicking on the corresponding button.

**Example 1:** on the healthpage, when clicking on "**Sensor Details**", nothing happens.

**Example 2:** in **Tools>Terminal** menu, when clicking on "**New modal terminal**", nothing happens.

**Solution:** It might be needed to configure Firefox to allow the display of pop-ups. by default, Firefox is blocking certain pop-ups, unless there is a specific exception defined by the user for the website. Follow the steps below to add an exception to allow pop-ups:

- Launch Firefox
- Display the Firefox menu (in the upper right part of the window by default)
- Select "**Preferences**"



- A Firefox preferences window opens. Select the "**Content**" tab.
- Click on the "**Exceptions**" button next to "**Block pop-up windows**".
- Enter the url of your AW Server in the "**address of website**" text field (e.g. "**localhost**" or "**127.0.0.1**" or "**10.10.0.45**")
- Click on "**Allow**". The url is added to the list of exceptions.
- Once you are done adding exceptions, click on "**Close**". Click on "**Close**" again.
- Refresh the page you were trying to display. Pop-ups are now allowed.

### 3.4.6.3 High Tier Load Failure

**Problem:**

After OS load, "Packages Completed" screen is displayed. However after reboot, an error message displays saying: "Media Failure Check Cable".

**Solution:**

The Boot order for DAS and High Tier is swapped.

To correct this:

1. Reboot the Server and enter BIOS Setup by pressing <**F9**> key during Boot sequence.
2. Select **Boot Controller Order <Enter>**.
3. Select **HP Smart Array P420i Controller <Enter>**.
4. Select **Controller Order 1 <Enter>**.
5. Exit BIOS Setup and save the parameters.

The Server should now correctly boot.

### 3.4.6.4 Backup/Restore compatibility issue with DICOM hosts

**Problem:**

During a software update or upgrade of a version prior to AWS3.2 Ext 2.0 to a version AWS3.2 (Ext 2.0, 3.0 or 3.2), the DICOM hosts are not properly restored. They are available in the Service Tools but are not visible on client.

The following files restored from previous version are not compatible with the new software version:

```
/export/home/sdc/nuevo/resources/network/network-cfg.xml
/export/home/sdc/nuevo/resources/browser/sessions.properties
```

**Solution:**

In this case, it is necessary to reinstall the files from the RPM package, from the platform media that was used for the installation, as follow:

1. Record the data of the DICOM hosts currently configured.
2. Put the AW Server in maintenance mode to avoid conflicts on files being used.
3. For each RPM package and the corresponding name and location in AWS:

| RPM Package                 | File/Directory Path in RPM                                                                                      | File/Directory Location in AWS                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| nuevo-config-CSERel<br>ease | ./thesource/dumpall/build_workpo<br>ol/job-868457/nuevoconfig/AWE/re<br>sources/network/network-cfg.xml         | /export/home/sdc/nuevo/resou<br>rces/network/network-cfg.xml         |
| nuevo-config-CSERel<br>ease | ./thesource/dumpall/build_workpo<br>ol/job-868457/nuevoconfig/AWE/re<br>sources/browser/sessions.propert<br>ies | /export/home/sdc/nuevo/resou<br>rces/browser/sessions.proper<br>ties |

Use the **rpm2cpio** command to extract the file/directory from the RPM package mentioned previously and copy them at the right location. See [A.23 RPM2CPIO on page 528](#) for the full procedure.

**NOTE**

The package name (first column) is truncated. The full name of the package contains the version.

**NOTE**

The job version (second column) may change depending on version.

**NOTE**

As the RPM package is the same for both rows, for the second row you can just start at [step 6](#) in [A.23 RPM2CPIO on page 528](#).

4. Change owner of the reinstalled files:

```
cd /export/home/sdc/nuevo/resources <Enter>
chown sdc:sdc network/network-cfg.xml <Enter>
chown sdc:sdc browser/sessions.properties <Enter>
```

5. Restart all services. Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#)
6. Reenter the DICOM hosts, previously recorded, from the Service Tools.

### 3.4.6.5 Logfile partition full

**Problem:** Logfile partition fill up with logfile content in AW Server 3.2 Ext. 2.0. Logrotate is the feature responsible for keeping the logfile contents in a healthy level, and delete the old content. The ~sdc/nuevo/logfiles/dicomserver.console.out logfile is not handled by logrotate and can fill up logfile partition.

**Solution:** To prevent this from happening the workaround is to update the ~sdc/nuevo/resources/system/nvologrotate.conf file as follow:

1. Open the AW Server Console/terminal, login as **root**.
2. Using any text editor open the file ~sdc/nuevo/resources/system/nvologrotate.conf

3. Replace the following lines in the file:

```
/export/home/sdc/nuevo/logfiles/nwscp.log {
rotate 10
size=10M
}
By
/export/home/sdc/nuevo/logfiles/dicomserver.console.out {
rotate 10
size=10M
copytruncate
}
```

4. In case the logfile partition is already filled up, the dicomserver.console.out file needs to be deleted. Type the following command in the terminal:

**rm ~sdc/nuevo/logfiles/dicomserver.console.out <Enter>**

5. Reboot the AW Server. Type the following command in the terminal:

**reboot <Enter>**

### 3.4.6.6 AW Server Client login fails due to DLL mistake

**Problem:** In some rare occasion, the X-Server cannot be launched due to DLLs mess caused by some other components installed on the windows client station. In this case, login fails and AWS Client logfile (%APPDATA%/Solo/<latest instance id>/logs/<latest global log>) contains Error compiling keymap and Server terminated with error (1). Closing log file. error messages.

Most of the time this kind of error is caused by some components or applications installed on the windows client station which pushes their DLLs in front of normal DLLs required by AW Server Client application (e.g: XWinGEAWE32.exe). In this case the normal behavior of some function is changed and AW Server cannot function.

**Solution:** To prevent this:

1. Review the DLLs list and check if unusual DLLs are present
2. Find the application or component which provides the DLLs
3. Uninstall the application from Windows.

#### NOTE

The following Microsoft tools can help to review the running processes and associated DLLs:

<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

#### NOTE

**To perform the above steps, please contact the OLC and the AW Engineering.**

### 3.4.6.7 Users disconnected following an unexpected CoLA License Server crash

This workaround is applicable for **AW Server 3.2 Ext. 3.0** release.

**Problem:**

- AW Server core services restart causing users to be disconnected
  - AW Server is temporarily unavailable
  - CoLA License Server is temporarily unreachable (not running)
  - Users are temporarily not able to launch application(s)
- All the applications are unavailable (grayed out as if they were not installed or activated)

**Diagnostic:**

To diagnose if the problem comes from the CoLA License Server, you must log in to the server and run the following command:

**ls -lt /var/log/gehc/cores/core.gemsLicenseServ.\* <Enter>**

- If this command returns an empty list, it means that there was no Cola crash and this workaround is not applicable.
  - If this command returns a list, this list shows coredump files resulting from Cola server crashes. Then you should apply the workaround described below.
- After that, further CoLA crashes will be reported in the **/var/log/messages** file.

**Solution:**

The solution consists of two major steps, first to exclude cola service supervision from the watchdog service, second to add a script that will restart the Cola service as soon as it fails.

1. Open a Terminal and login as **root**.
2. Create the following script that will immediately restart CoLA License Server in case of crash:
  - a. Type:  
**cd /usr/share/FL\_Server <Enter>**  
**nano -c gemsLicenseServer.sh <Enter>**

- b. Copy the text inside the following box using **<CTRL> + <C>** keys:

```
#!/bin/bash
CAL_HOME="/usr/share/FL_Server/"
COLA_SERV_NAME="Floating License Server"
COLA_USER=gehc_security
while [true]
do
logger "Starting $COLA_SERV_NAME"
su - ${COLA_USER} -c "$CAL_HOME/gemsLicenseServer" > ${CAL_HOME}/licenseserver.out 2>&1
logger "CoLA crashed, restarting."
done
```

- c. Click in the terminal window and paste the text using **<Shift> + <Insert>** keys for nano editor.
- d. Press **<Ctrl> + <X>** to save the file and exit.
- e. Type "Y" to confirm and press **<Enter>** to validate the file name.
- f. Type:

**chmod +x gemsLicenseServer.sh <Enter>**

**NOTE**

You can edit the files listed below using the nano editor or any suitable editor such as vi.

3. Stop watchdog to avoid restart of services when editing configuration scripts.

- a. Type:

**/etc/init.d/watchdog stop <Enter>**

- b. Make sure that watchdog is no longer running (it can take up to two minutes for the service to stop):

**/etc/init.d/watchdog status <Enter>**

Checking for service WatchDog: not running

4. Stop cola service.

- a. Type:

**/etc/init.d/cola stop <Enter>**

- b. Make sure that cola is no longer running:

**/etc/init.d/cola status <Enter>**

Checking Floating License Server: CoLA\_License\_Server;node-locked[...] not running

5. Edit "cola" file so that it calls for the script mentioned above to start the CoLA License Server.

Type:

**cd /etc/init.d <Enter>**

**nano -c cola <Enter>**

- a. **Line 36**, change:

"ps ax | grep gemsLicenseServer | grep -v grep | awk '{ print \$1 }' | head -n 1"

to

"ps ax | grep gemsLicenseServer | grep gehc\_security | grep -v grep | awk '{ print \$1 }' | head -n 1"

- b. **Line 49**, change:

"su - \${COLA\_USER} -c "\${CAL\_HOME}/gemsLicenseServer" > \${CAL\_HOME}/licenseserver.out 2>&1 &"

to

"su - \${COLA\_USER} -c "\${CAL\_HOME}/gemsLicenseServer.sh" &"

- c. **Line 72**, change:

"kill \${COLA\_SERVER\_PID}"

to

"pkill gemsLicenseS"

- d. Press **<Ctrl> + <X>** to save the file and exit.

- e. Type "Y" to confirm and press **<Enter>** to validate the file name.

6. To remove licenseserver.out file and restart cola service, type:

**rm -rf /usr/share/FL\_Server/licenseserver.out <Enter>**

**/etc/init.d/cola start <Enter>**

Starting Floating License Server: OK

7. Edit "service-list.xml" file to remove CoLA License Server restart conditions and restart watchdog.

a. Type:

```
cd /var/lib/ServiceTools/conf <Enter>
```

```
nano -c service-list.xml <Enter>
```

b. **Lines 327 to 329**, comment out the lines:

```
<!-- <RestartCondition>/usr/share/ServiceTools_AWS/scripts/cola/get_server_key.sh </
RestartCondition>
```

```
<RestartConditionFromHP>/usr/share/ServiceTools_AWS/scripts/cola/get_server_key.sh</
RestartConditionFromHP> -->
```

c. Press **<Ctrl> + <X>** to save the file and exit

d. Type "Y" to confirm and press **<Enter>** to validate the file name.

e. To restart watchdog, type:

```
/etc/init.d/watchdog start <Enter>
```

8. To check the PIDs (Process ID) of gemsLicenseServer related processes, type:

```
ps -ef | grep gemsLicense | grep -v grep | grep -v su <Enter>
```

Example of output:

```
501 8059 8057 0 07:50 ? 00:00:00 /bin/bash /usr/share/FL_Server//
gemsLicenseServer.sh
```

```
501 13621 8059 0 07:54 ? 00:00:00 /usr/share/FL_Server//
gemsLicenseServer
```

Both processes should run with gems\_security (501) user.

### 3.4.6.8 Remote node control enabled

This workaround is applicable for **AW Server 3.2 Ext. 3.2** release.

**Problem:** AWS 3.2 Ext. 3.2 has node control ENABLED by default and CANNOT be deactivated from Service Tools. It means that the DICOM hosts that have not been declared on the AW Server are not allowed to query/retrieve images from the AW Server and to store images to the AW Server.

This is a major change versus the previous AW Server release and may cause issues during upgrades, if undeclared DICOM hosts push to or retrieve from the AW Server.

**Solution:** To avoid connectivity issues for undeclared DICOM hosts:

- **Declare the DICOM Hosts**

Declare all DICOM host communicating with AW Server as described in the AW Server 3.2 Installation and Service Manual, Job Card IST010 - Administrative Configuration.

**NOTE**

Keep the three following checkboxes on the DICOM host configuration page checked by default:



OR

- **Disable the node control as follows:**

1. Open the AW Server Console/terminal, login to the AW Server as **root**.
2. Using any text editor open the file `/export/home/sdc/nuevo/scripts/startup/startDicomServer`
3. Insert the following line below line containing `# unset DisableNodeValidation env` variable to enable Node Validation:  
`export DisableNodeValidation=true`
4. Restart all services from the Service Tools Health Page.  
Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#).

### 3.4.6.9 Unexpected network traffic sent from AW Server

**Problem:** On AW Server 3.2 Ext. 3.2 the Operating System performs periodic check for updates on the DNS servers. From customer point of view, this periodic check can appear as unexpected network traffic or unexpected TCP/IP packages sent from the AW Server to the DNS servers.

**Solution:** To avoid unexpected network traffic, comment out the content of the `/etc/cron.d/unbound-anchor` file as follow:

1. Put the AW Server in maintenance mode, to guarantee there is no user connected to server, as a restart will be necessary.
2. Open the AW Server Console/terminal, login as **root**.
3. Comment out the content of the unbound-anchor file. Type the following commands in the terminal:  
`cp /etc/cron.d/unbound-anchor /etc/cron.d/unbound-anchor.orig <Enter>`  
`sed -i 's/^#/' /etc/cron.d/unbound-anchor <Enter>`
4. Reboot the AW Server. Type the following command in the terminal:  
`reboot <Enter>`
5. Once reboot is complete, exit the maintenance mode.

### 3.4.6.10 Incoming DICOM transfer attempts fail

**Problem:** On AW Server 3.2Ext. 3.2, the DICOM communication service leaks system resources (too many open files), and over time it can use up to all available resources and result to DICOM communication service failure (incoming DICOM associations are rejected).

**Diagnostic:** To diagnose if the problem actually comes from the issue described above and not from other kind of DICOM communication errors, run the following command:

1. Open the AW Server Console/terminal, login as **root**.
2. Type the following commands:

```
cd /var/log/gehc/sdc/nuevo/logfiles <Enter>
cat dicomserver.log | grep -i "Too many open files" <Enter>
```

You should get the following result:

```
java.io.FileNotFoundException: /export/home/sdc/nuevo/resources/i18n/
UserMessages.properties (Too many open files)
```

**Detection:** When the root cause (resource leak) is at play the number of files open for DicomServer component increases permanently over time. You can check this with the following procedure:

1. In the terminal, get the dicomserver process PID as follow, and note it:

```
pgrep -f com.ge.hc.nuevo.dicom.net.scp.server.DicomServer <Enter>
```

2. Execute the below commands (replace <PID> by the result of the above command) and check the result numbers (the result of these commands shall be below **10**):

```
ls -l /proc/<PID>/fd | grep "UserMessages.properties" | wc -l <Enter>
```

```
ls -l /proc/<PID>/fd | grep "masterexternal.properties" | wc -l <Enter>
```

**Solution:** The workaround, to recover the resources used by the DICOM communication service, consists of 2 parts, described below:

1. Increase the number of available file descriptors (files open) available for processes of **sdc** user (by default to 10000) to prevent the issue from happening with high frequency (shall be less than daily, optimally less than weekly):

- a. Put the AW Server in maintenance mode, to guarantee there is no user connected to server, as a restart will be necessary.
- b. Open the AW Server Console/terminal, login as **root**.
- c. Check the threshold value of available file descriptors for the DicomServer component:

- Get the dicomserver process PID as follow, and note it:

```
pgrep -f com.ge.hc.nuevo.dicom.net.scp.server.DicomServer <Enter>
```

- Execute the below command (replace <PID> by the result of the above command):

```
cat /proc/<PID>/limits | grep "Max open files" <Enter>
```

Output is like:

```
Max open files 4096 4096 files
```

- d. Add a line to increase the threshold of available file descriptors, at the end of the /etc/security/limits.conf file, as follow:

```
/bin/cp /etc/security/limits.conf /etc/security/limits.conf_orig <Enter>
```

```
echo -e "sdc - nofile 10000\n" >> /etc/security/limits.conf <Enter>
```

- e. Reboot the AW Server. Type the following command in the terminal:

```
reboot <Enter>
```

- f. Once reboot is complete, check the threshold value change for the DicomServer component:

Proceed as in substep [Step 1.c](#) above.

Output shall be:

```
Max open files 10000 10000 files
```

- g. Exit the maintenance mode.

#### NOTE

Side effect: Server performance degradation, or server failure under extremely high system load.

2. Automate reoccurring scheduled restart of the DICOM (SCP) communication service to prevent from reaching the maximum number of open files threshold. For this a script shall be created and deployed to the server and customized for the local needs. Create the script file as follow:

- a. Open the AW Server Console/terminal, login as **root**.

- b. In the terminal, create the directory that will receive the file and navigate to this directory:

```
mkdir /usr/share/ServiceTools_AWS/scripts/workaround <Enter>
```

```
cd /usr/share/ServiceTools_AWS/scripts/workaround <Enter>
```

- c. Open the script file (dicomserver\_restart.sh):

```
vi dicomserver_restart.sh <Enter>
```

Press the **<i>** key to edit the file.

- d. Copy/paste the text, inside the following box, to the file:

```
#!/bin/bash
readonly threshold=5000
readonly pid=$(pgrep -f com.ge.hc.nuevo.dicom.net.scp.server.DicomServer)
readonly fd_num=$(ls -l /proc/$pid/fd | wc -l)
echo "$(date) dicomserver PID: $pid FD amount: $fd_num"
if [[$fd_num -ge $threshold]]; then
echo "Restarting dicomserver"
kill -15 $pid
sleep 10
readonly newpid=$(pgrep -f com.ge.hc.nuevo.dicom.net.scp.server.DicomServer)
echo "$(date) dicomserver oldPID: $pid newPID: $newpid"
if [[$pid -ne $newpid]]; then
echo "success"
else
echo "terminate failure, kill attempt"
kill -9 $pid
sleep 10
readonly newpid2=$(pgrep -f com.ge.hc.nuevo.dicom.net.scp.server.DicomServer)
echo "$(date) dicomserver oldPID: $pid newPID: $newpid2"
if [[$pid -ne $newpid2]]; then
echo "success by kill"
else
echo "kill failure"
fi
fi
fi
```

- e. Press **<Enter>** to add an empty line at the end of the file.

- f. Press **<Esc>** then **:wq** to save the file and exit.

- g. Give executable rights to the file:

```
chmod 755 dicomserver_restart.sh <Enter>
```

- h. Configure the cron table file that specifies commands/scripts to run periodically on a given schedule, with the above script:

- Open the cron table file:

```
crontab -e <Enter>
```

- The cron table file opens using "vi" editor. Go to the end of the file using the **<Down arrow>** key then press the **<o>** key to insert a line in the file.

- Copy/paste the line, inside the following box, to the end of the cron table file:

```
20 2 * * * /usr/share/ServiceTools_AWS/scripts/workaround/
dicomserver_restart.sh
```

#### NOTE

Side effect: When triggered, this script (`dicomserver_restart.sh`) can result in communication breakage if there is incoming DICOM communication, causing incomplete dataset transfer in case broken communication is not attempted again at a later time.

- Press `<Esc>` then `:wq` to save the file and exit.
- Verify the content is as intended in crontab configuration by typing  
`crontab -l <Enter>`

The line(s) added above should be present in the output of the command.

- i. Verify the correctness and functionality of the script:

Perform the below steps during an idle time period of the server from DICOM incoming traffic perspective.

- Open the AW Server Console/terminal, login as `root`.
- Run the script from the terminal, as follow:

```
cd /usr/share/ServiceTools_AWS/scripts/workaround <Enter>
sh dicomserver_restart.sh <Enter>
```

It should give back output similar to this:

```
Fri Sep 13 02:13:25 CEST 2019 dicomserver PID: 4582 FD amount: 67
```

- Edit the “threshold” value in the script from default to a small number (50), to be able to trigger the actual functionality, and run the script (will run for 10 seconds):

```
/bin/cp dicomserver_restart.sh dicomserver_restart.sh_orig <Enter>
sed -i 's/readonly threshold=.*$/readonly threshold=50/' \
dicomserver_restart.sh <Enter>
sh dicomserver_restart.sh <Enter>
```

It should give back output similar to this:

```
Fri Sep 13 02:17:03 CEST 2019 dicomserver PID: 4582 FD amount: 67
Restarting dicomserver
Fri Sep 13 02:17:13 CEST 2019 dicomserver oldPID: 4582 newPID:
10766
Success
```

- Change back the threshold value to the default value:

```
/bin/cp dicomserver_restart.sh_orig dicomserver_restart.sh <Enter>
```

### 3.4.6.11 Cannot save Postscript printer when the IP address contains a 0

**Problem:** On AW Server 3.2 a Postscript printer configured with an IP address containing a “0”, in one of the four decimal numbers, cannot be saved/added (for instance, IP: 3.249.0.34).

**Solution:** Do not used “0” in one of the four decimal numbers of the IP address when configuring a Postscript printer.

**NOTE**

The four decimal numbers available range is [0-255]. In AW Server 3.2 Ext. 3.2 do not use the “0”.

### 3.4.6.12 Hard drives check command not working on HPE ProLiant DL360 Gen9 Server

**Problem:** When attempting to check hard drives using the disk/array controller command an error is displayed as illustrated below:

```
hpssacli ctrl all show config
```

```
Smart Array P440ar in Slot 0
(Embedded)
```

```
APPLICATION UPGRADE REQUIRED:
```

```
This controller has been configured with a more recent version of software.
To prevent data loss, configuration changes to this controller are not
allowed.
```

```
Please upgrade to the latest version to be able to continue to configure
this controller.
```

This message indicates that the command is outdated and needs to be updated.

**Solution:** Use the command `ssacli`:

- From your laptop, open the HP support portal: [https://support.hpe.com/hpsc/swd/public/detail?swItemID=MTX\\_e5e206634500467b9121f977cf#tab3](https://support.hpe.com/hpsc/swd/public/detail?swItemID=MTX_e5e206634500467b9121f977cf#tab3).

Hewlett Packard Enterprise Support Center

 [Printable version](#)

## Drivers & software

### HPE Smart Storage Administrator (HPE SSA) CLI for Linux 64-bit

By downloading, you agree to the terms and conditions of the [Hewlett Packard Enterprise Software License Agreement](#).

**Note:** Some software requires a valid warranty, current Hewlett Packard Enterprise support contract, or a license fee.

|                            |                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type:                      | Software - System Management                                                                                                                                                                                                                |
| Version:                   | 4.15.6.0(20 Dec 2019)                                                                                                                                                                                                                       |
| Operating System(s):       | Red Hat Enterprise Linux 6 Server (x86-64)<br>Red Hat Enterprise Linux 7 Server<br>Red Hat Enterprise Linux 8 Server<br>SUSE Linux Enterprise Server 11 (AMD64/EM64T)<br>SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server 15 |
| <b>Multi-part download</b> |                                                                                                                                                                                                                                             |
| File name:                 | <a href="#">ssacli-4.15-6.0.x86_64.compsig (2.0 KB)</a>                                                                                                                                                                                     |
| File name:                 | <a href="#">ssacli-4.15-6.0.x86_64.rpm (15 MB)</a>                                                                                                                                                                                          |
| File name:                 | <a href="#">ssacli-4.15-6.0.x86_64.txt (7.5 KB)</a>                                                                                                                                                                                         |

|                          |
|--------------------------|
| <a href="#">Download</a> |
| <a href="#">Download</a> |
| <a href="#">Download</a> |

- Select the `ssacli-4.15-6.0.x86_64.rpm` RPM package and download it.
- Upload the RPM package to the AW Server using the file transfer tool from the Service Tools in **Tools > File Transfer**.
- Open the AW Server Console/terminal and login as `root`.
- Remove the former `hpssacli` command:

```
rpm -e hpssacli <Enter>
```

- Install the `ssacli` command:

```
rpm -ivh /var/lib/ServiceTools/upload/ssacli-4.15-6.0.x86_64.rpm
```

7. Check hard drives:

```
ssaci ctrl all show config
```

It returns the disk/array controller data without error message.

### 3.4.6.13 DICOM requests (C-FIND) character representation not supported by older systems

**Problem:** AW Server sends DICOM requests (C-FIND) in ISO\_IR 192 character representation. This is not supported by some older PACS and DICOM systems and can result in unavailable DICOM communication with these systems.

**Solution:** To avoid DICOM communication issues, update the DICOM charset to ISO\_IR 100 in the AW Server settings:

1. Open the AW Server Console/terminal, login as **root**.
2. Type the following commands:

```
cd ~sdc/nuevo <Enter>
```

```
echo "setenv DICOM_CHARSET 'ISO_IR 100'" >> .nuevorc <Enter>
```

3. Restart all services.

Refer to [3.4.1.8 Software Subsystem Restart on page 164](#).

### 3.4.6.14 AW Server Client login fail due to display error

**Problem:** When attempting to logging into AW Server Client from a Windows 7 computer, a display error appears (`Local display could not be initialized`) and the login is blocked. This is caused by OpenGL resources conflict on the Windows 7 computers.

**Solution:** To avoid the display error, update the script `startx.bat` which starts the AW Server Client:

1. Open the file (`C:\Program Files (x86)\GE\AWS_3.2\solo\nx\startx.bat`) in the Notepad editor.
2. At the end of the line starting by `CALL XWinGEAWE32`, add `-nowgl` as shown below.

```
CALL XWinGEAWE32 %XWINDISPLAY% -nolock -cc 24 -logverbose 1 -extension Composite -logfile %TMPDIR%/X.log -notrayicon -noreset %WINDOWMODE% -mwallowembed -swcursor -xkkdir ./ -fp fonts/75dpi,fonts/100dpi,fonts/misc -nowgl
```

Logging into AW Server Client works again.

### 3.4.6.15 EA3 authentication using SSL connection with Active Directory not working

**Problem:** On AW Server 3.2 Ext. 3.4 and higher, the EA3 authentication failed (**Test Connection** failed) if the **Server Name / IP** contains the Active Directory IP and the SSL protocol is selected. This is due to the recent Java versions which enable the Endpoint identification on LDAP connections.

**Solution:** To avoid this issue, fill the **Server Name / IP** with the Active Directory Server **certificate Common Name** (also called **FQDN** (Fully Qualified Domain Name)):

1. Open the AW Server Console/terminal and login as **root**.
2. Type the command:

```
openssl s_client -connect <Active Directory IP>:636 | grep -i CONTROLLER
```

The following lines display:

```
0 s:/CN=<FQDN>/OU=DOMAIN-CONTROLLER/OU=MULTI-ALLOWED
subject=/CN=<FQDN>/OU=DOMAIN-CONTROLLER/OU=MULTI-ALLOWED
```

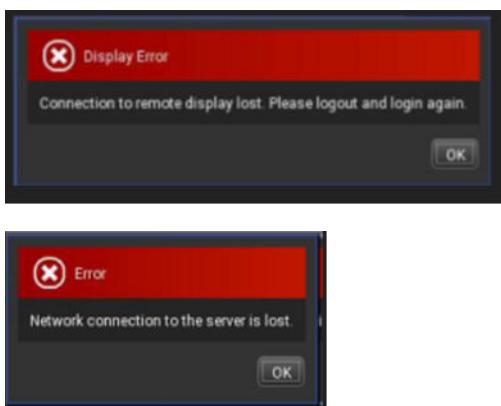
For instance:

```
0 s:/CN=DCCINOHP0103.logon.ds.ge.com/OU=DOMAIN-CONTROLLER/OU=MULTI-
ALLOWED
subject=/CN=DCCINOHP0103.logon.ds.ge.com/OU=DOMAIN-CONTROLLER/OU=MULTI-
ALLOWED
```

3. Copy the Active Directory Server **certificate Common Name** (CN), from the <FQDN> into the **Server Name / IP** field.
4. Resume from step 1 in the *Configuration Instructions* panel.

### 3.4.6.16 AW Server Client connection with the AW Server is lost

**Problem:** The AW Server Client connection with the AW Server is lost and the following connection errors appear:



This issue occurs when the connection between the AW Server Client and the AW Server is a secure connection. This secure connection is kept alive by the httpd server, till a user is logged. Then, the log rotation function tries to access the same system resources as the httpd server, which leads to restart the httpd server and to interrupt the secure connection.

**Solution:** To avoid this issue, update the httpd logrotate configuration file to disable the httpd server restart:

1. Open the AW Server Console/terminal and login as **root**.
2. Navigate to the `/etc/logrotate.d` directory:

```
cd /etc/logrotate.d <Enter>
```

3. Make a copy of the `httpd` file:

```
mkdir /etc/logrotate.d.backup <Enter>
```

```
cp httpd /etc/logrotate.d.backup <Enter>
```

4. Modify the `httpd` file:

```
sed -i 's/missingok/missingok\n copytruncate/' httpd <Enter>
```

```
sed -i -e '/postrotate/d' -e '/reload/d' -e '/endscript/d' httpd <Enter>
```

5. Verify that the `httpd` file contains the following lines:

```
cat httpd <Enter>
```

```
/var/log/httpd/*log {
 missingok
 copytruncate
 notifempty
 sharedscripts
 delaycompress
}
```

6. Restart all services.

Refer to [3.4.1.8 Software Subsystem Restart on page 164](#).

### 3.4.6.17 Updating the AE Title following the hostname characters policy change in OS 6.0 (HeliOS 7.7)

**Problem:** From AW Server 3.2 Ext. 4.0, the hostname characters policy changes with the OS 6.0 (HeliOS 7.7). The underscore ( \_ ) and the upper case characters ([A-Z]) are not allowed anymore in the hostname whereas the AE Title authorize these characters. By default, the AE Title of an AW Server is set to the hostname value. In case of an AW Server upgrade, this can lead to inconsistency of the AE Titles between the AW Servers and the remote DICOM nodes at other Medical Devices (AW Servers configured on remote systems).

For instance, if the hostname and the AE Title of an AW Server is AWS\_Node1, during an upgrade of the AW Server, the hostname must be changed (to `awsnode1` for instance). If this AW Server is configured as a remote DICOM node at other Medical Devices, the AE Title must be changed on all these systems.

**Solution:** To avoid having to change the AE Title on all Medical Devices, change the AE Title separately from the hostname on the AW Server:

1. Open the AW Server Console/terminal and login as `root`.

2. Navigate to the `/export/home/sdc/nuevo/resources/network` directory:

```
cd /export/home/sdc/nuevo/resources/network <Enter>
```

3. Add the AE Title of the AW Server (e.g.: the hostname before the upgrade) in the `network-cfg.xml` file:

```
cp network-cfg.xml network-cfg.xml.orig <Enter>
```

```
sed -i 's/^(^ *<DicomAppSettings>.*\')/\1\n <AETitle>AWS_Node1<\/
AETitle>/' network-cfg.xml <Enter>
```

where `AWS_Node1` is the hostname before upgrade.

4. Verify that the AE Title is added to the `network-cfg.xml` file:

```
diff network-cfg.xml network-cfg.xml.orig <Enter>
```

The following line appears:

```
> <AETitle>AWS_Node1</AETitle>
```

5. Reboot the AW Server:

```
reboot <Enter>
```

### 3.4.6.18 CoLA server not running after software update or system reboot

**Problem:** After completing an update (Load From Cold, restoration of the previous AW Server system configuration, platform license setup ...) to an AW Server 3.2 Ext. 3.4 from a previous AW Server, the CoLA server does not start (or does not start properly) after the AW Server reboot (even after a second reboot). Thus, no Floating license is available and the applications cannot be started.

**Solution:** To eliminate this issue, update the CoLA service script then stop the running CoLA process and restart it:

1. Open the AW Server Console/terminal and login as **root**.

2. Navigate to the /etc/init.d directory:

```
cd /etc/init.d <Enter>
```

3. Backup the cola file:

```
cp cola cola.orig <Enter>
```

4. Update the cola file:

```
sed -i 's/\\(ps ax .*runuser \\)\\(.*$\\)/\\1| grep -v CAL_HOME \\2/g' cola <Enter>
```

5. Verify that the cola file is updated correctly:

```
diff cola cola.orig <Enter>
```

The following lines appear:

```
< ps ax | grep gemsLicenseServer | grep -v grep | grep -v bash | grep -v /sbin/runuser | grep -v CAL_HOME | grep -v CAL_HOME | awk '{ print $1 }' | head -n 1
```

```

```

```
> ps ax | grep gemsLicenseServer | grep -v grep | grep -v bash | grep -v /sbin/runuser | grep -v CAL_HOME | awk '{ print $1 }' | head -n 1
```

6. Stop the CoLA process twice:

```
/bin/sh /etc/init.d/cola stop <Enter>
```

```
/bin/sh /etc/init.d/cola stop <Enter>
```

7. The CoLA process is started automatically by a watchdog service after 120 seconds delay, if watchdog service is running:

- a. Check if watchdog service is running:

```
ps -ef | grep watchdog.sh <Enter>
```

The output of the command should be:

```
root 6969 1 0 21:40 pts/0 00:00:00 /bin/bash /usr/share/ServiceTools/scripts/coreWatchDog/watchdog.sh -f /var/lib/ServiceTools/conf/service-list.xml
```

```
root 7848 21619 0 21:40 pts/0 00:00:00 grep watchdog.sh
```

- b. If the watchdog service is not running (in Step 7.a only the second line appears), start it:

```
/etc/init.d/watchdog start <Enter>
```

The output of the command should be:

```
Starting WatchDog 6969
```

```
OK
```

- c. If the output of the command in Step 7.b is:

```
Starting WatchDog /usr/share/ServiceTools/scripts/coreWatchDog/watchdog.sh Error: Lock file is in place
```

Make sure an old instance of this program is not running, remove it and try again.

Could not start WatchDog

Remove the lock file and start the watchdog service again:

```
rm -rf /tmp/watchdog.lock <Enter>
/etc/init.d/watchdog start <Enter>
```

8. Wait for the CoLA process to restart by checking the watchdog log file:

```
tail -f /var/lib/ServiceTools/log/watchdog/watchdog.log <Enter>
```

The following lines appear when the CoLA process restarts:

```
Wed Dec 2 18:10:23 CET 2020: echo /etc/init.d/cola :Not running, need to
restart.
```

```
Wed Dec 2 18:10:23 CET 2020: echo /usr/share/ServiceTools/scripts/
xpreproc/xpreprocWatchdogStatus.sh :Not running, need to restart.
```

```
Wed Dec 2 18:10:32 CET 2020: restart all services
```

9. Type **<Ctrl> <c>** to exit the command.

### 3.4.6.19 Restore fails if the built-in Floating License server (CoLA) is disabled

**Problem:** On any AW Server, if the System Configuration is backed-up with the built-in CoLA licensing disabled and external licensing servers are configured, the restoration of the Licensing configuration on an AW Server 3.2 Ext. 4.0 fails. Restore is interrupted at the licensing restoration.

**Solution:** To avoid having this issue, update the file used to restore the license server configuration and perform restoration again.

1. Open the AW Server Console/terminal and login as **root**.

2. Navigate to the `/usr/share/ServiceTools/scripts/backuprestore` directory:

```
cd /usr/share/ServiceTools/scripts/backuprestore <Enter>
```

3. Update the `post_restore_licensing.sh` file:

```
cp post_restore_licensing.sh post_restore_licensing.sh.orig <Enter>
sed -i 's/^(CoLA_License_Server)/\1 || [[\$? == 1]] /g' \
post_restore_licensing.sh <Enter>
```

4. Verify that the `post_restore_licensing.sh` file is updated correctly:

```
diff post_restore_licensing.sh post_restore_licensing.sh.orig | head -2
<Enter>
```

The following line appears:

```
< licenseExist=$(./usr/bin/licenseAdmin -llist | grep
CoLA_License_Server || [[\$? == 1]] | awk -F\; "\{print \$4\}")
```

5. Reboot the AW server:

```
reboot <Enter>
```

6. Restore the system configuration again from Service Tools.

### 3.4.6.20 Norwegian language support for Solo Client on AW Server Seamless integration mode

**Problem:** On the AW Server 3.2 Ext. 3.4, in Seamless integration mode, even though the UV is set to Norwegian language, the Solo Client remains in English.

**Solution:** To avoid having this issue, perform the following steps:

1. Close the Solo Client.
2. At the client PC, open a Command Prompt window.
3. Navigate to the `C:\Program Files (x86)\Integrad.3\MIV\Solomini\aws3.2-3.4` directory:

```
cd "C:\Program Files (x86)\Integrad.3\MIV\Solomini\aws3.2-3.4" <Enter>
```

4. Edit the `solomini.ini` file with Notepad editor.

Insert the following lines between line `-clean` and line `-vmargs`:

```
-nl
```

```
no_NO
```

The `solomini.ini` file should contain the following lines:

```
-clean
```

```
-nl
```

```
no_NO
```

```
-vmargs
```

```
-Djsse.enableSNIExtension=false
```

5. Start the Solo Client.

### 3.4.6.21 DICOM Direct Connect performance issues

**Problem:** In DICOM Direct Connect integration mode, the AW Server 3.2 Ext 4.0 encountered performance issues. Especially when loading MR studies.

**Solution:** To avoid those performances issues, update the DICOM Direct Connect settings:

1. Open the AW Server Console/terminal and login as `root`.

2. Stop the DICOM Direct Connect service:

```
systemctl stop tomcat@ddc <Enter>
```

3. Navigate to the `/var/lib/tomcats/ddc/conf` directory:

```
cd /var/lib/tomcats/ddc/conf <Enter>
```

4. Update the `service.properties` file:

```
cp service.properties service.properties.orig <Enter>
```

```
sed -i 's/(\ddc.imageLevelThreshold=\.).*/\14/' service.properties <Enter>
```

5. Verify that the `service.properties` file is updated correctly:

```
diff service.properties service.properties.orig | \
```

```
grep ddc.imageLevelThreshold | head -1 <Enter>
```

The following line appears:

```
< ddc.imageLevelThreshold=4
6. Start the DICOM Direct Connect service:
systemctl start tomcat@ddc <Enter>
```

### 3.4.6.22 Cluster certificate application issue

**Problem:** On the AW Server 3.2 Ext 4.0, certificate application fails during cluster installation if AW Server time zone is behind UTC.

This issue occurs when executing the steps in Job Card IST012 - Virtual Servers Cluster Configuration, Certificate Management, in the AW Server 3.2 Ext. 4.0 Installation and Service Manual.

**Solution:** While executing the steps in Job Card IST012 - Virtual Servers Cluster Configuration, Certificate Management, once the certificate has been generated, update the script used to apply the certificate, then reapply the certificate on each node (AW Server) and the two HAPS of the cluster.

Execute [Step 1](#) to [Step 6](#) on the two HAPS first (start by the HAPS with lower IP), then on each node (in any order). And at last, execute [Step 7](#):

1. Open the AW Server Console/terminal and login as **root**.
2. Navigate to the `/root/certificate-management` directory:

```
cd /root/certificate-management <Enter>
3. Update the awsCert.py file:
cp awsCert.py awsCert.py.orig <Enter>
sed -i 's/(\^.*cert.start_time.*$)/#\1/' awsCert.py <Enter>
```

4. Verify that the awsCert.py file is updated correctly:

```
diff awsCert.py awsCert.py.orig | head -2 <Enter>
```

The following line appears:

```
< # cert.start_time <= datetime.now() or self._raise("{} is still not
valid".format(cert.name))
```

5. Apply the certificate with the following command:

```
/root/certificate-management/awsCert apply <Provider_IP> <Enter>
```

where `<Provider_IP>` is the IP of the node in which the certificate has been generated ("certificate provider").

For instance: `/root/certificate-management/awsCert apply 3.249.70.241`

The command requests a passphrase.

6. Enter the passphrase noted down when the certificate has been generated (in Job Card IST012 - Virtual Servers Cluster Configuration, Certificate Management).
7. In case of an HAPS, verify that the three following services are running:

```
systemctl status hws-service glusterd clb-service <Enter>
```

The following line within the result of the command should appear three times (one per service):

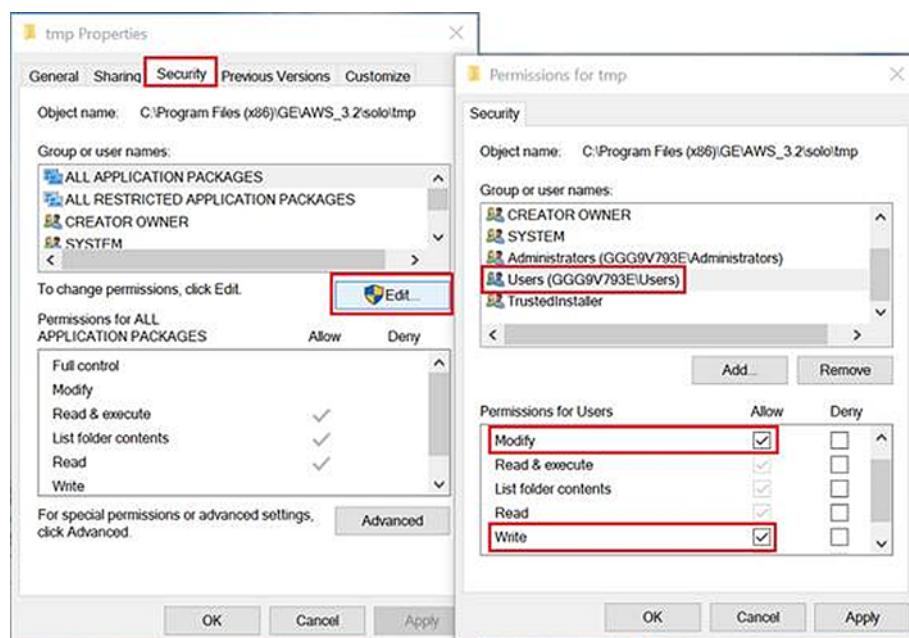
```
Active: active (running) since...
```

### 3.4.6.23 AW Server Client applications cannot start due to inappropriate user rights on Windows

**Problem:** When attempting to log into the AW Server Client from a Windows 7 or 10 computer, as a standard user, a display error message appears (Local display could not be initialized). The login succeeds when the message is clicked away, however, in the worklist, no image can be viewed and no application can be started. This is caused by inappropriate user rights on a folder on Windows. These folder rights are changed with the administrator rights if the AW Server Client is started once with these administrator rights. Then other users can no longer start the AW Server Client applications.

**Solution:** To avoid this issue follow the below workaround applicable for Windows 7 and 10:

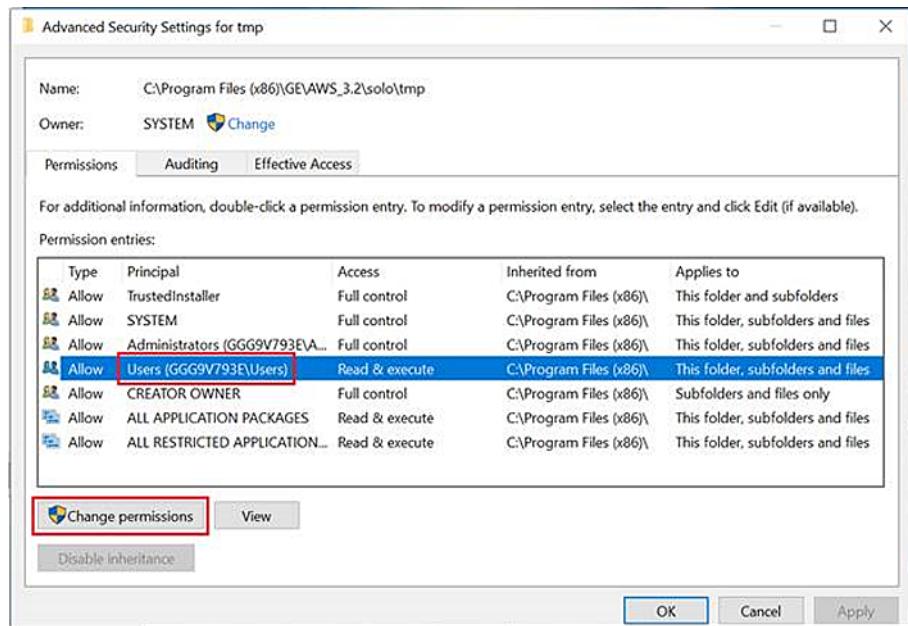
1. In a Windows Explorer, locate the C:\Program Files\GE\AWS\_3.2\solo\nx\tmp (or the C:\Program Files (x86)\GE\AWS\_3.2\solo\tmp) folder.
2. Right-click this folder and select **Properties**.
3. In the **Properties** window, select the **Security** tab and click **Edit** button.



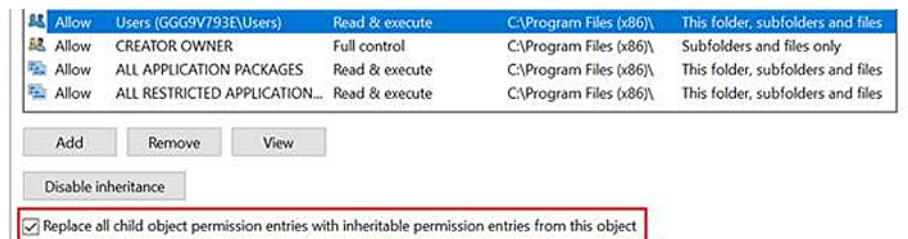
4. In the **Permission** window select the standard *Users* group, check the **Modify** and **Write** permissions and click on **OK**.
5. In the **Properties** window, select the standard *Users* group and verify that the **Modify** and **Write** permissions are checked.

|                      | Permissions for Users | Allow | Deny |
|----------------------|-----------------------|-------|------|
| Full control         |                       |       |      |
| Modify               | ✓                     |       |      |
| Read & execute       | ✓                     |       |      |
| List folder contents | ✓                     |       |      |
| Read                 | ✓                     |       |      |
| Write                | ✓                     |       |      |

6. In the **Properties** window, click on **Advanced** button and in the **Advanced Security Settings** window select the standard *Users* group and click on **Change permissions** button.



7. In the **Advanced Security Settings** window select the standard *Users* group again and check **Replace all child object permissions with inheritable permissions from this object**.



8. In the **Advanced Security Settings** window click on **OK** and acknowledge the popup that displays.  
 9. In the **Properties** window click on **OK**.

#### NOTE

This workaround will need to be reapplied if a new AW Server Client is installed. Unless a security policy is created, by the Customer IT Admin, to prevent the ~/nx/tmp folder creation after AW Server Client Installation.

### 3.4.6.24 Outgoing DICOM communication failure (C-FIND, C-STORE)

**Problem:** DICOM remote query (C-FIND SCU) might give back empty result, and/or copy to local (C-MOVE SCU) and send to (C-STORE SCU) services might fail (The End Of Review feature can be impacted also). This can be due to wrong ownership of some log files used by the DICOM SCU feature. Problem might be triggered by the **Administrative > Configuration > DICOM Hosts** configuration page, when using the **Check DICOM** button (DICOM test (C-ECHO SCU) feature).

**Detection:** To check that the issue faced is the one described above, review the log files as follow:

1. Open the AW Server Console/terminal, login as **root**.
2. For the symptom of empty DICOM remote query result (C-FIND SCU):

Review the /var/log/gehc/sdc/logfiles/awerun.log log file. Type the command:

---

```
less /var/log/gehc/sdc/logfiles/awerun.log <Enter>
```

The following such lines are present:

```
[TIMESTAMP]
com.ge.med.solo.patientlist.table.AbstractDmPatientListDataSource
runTask

SEVERE: An exception occurred while updating the model at exam level
java.lang.NullPointerException
at
com.ge.hc.nuevo.sessions.network.DicomAssociation.send(DicomAssociation.
java:523)
at
com.ge.hc.nuevo.sessions.network.NetworkSession.sendDicomQueryRequest(Ne
tworkSession.java:1599)
```

#### **NOTE**

Press the **<Space>** bar to scroll down in the file.

3. For the symptom of push (send to) and retrieve (copy to local) (C-STORE and C-MOVE SCU):

Review the `/export/home/sdc/nuevo/logfiles/serviceProvider.log` log file. Type the command:

```
less /export/home/sdc/nuevo/logfiles/serviceProvider.log <Enter>
```

The following such lines are present:

```
[TIMESTAMP] com.ge.hc.nuevo.sessions.network.NetworkSession
pushDicomStream

SEVERE: Corrupt Composite
java.lang.NullPointerException
at
com.ge.hc.nuevo.sessions.network.DicomAssociation.send(DicomAssociation.
java:523)
at
com.ge.hc.nuevo.sessions.network.NetworkSession.pushDicomStream(Networks
ession.java:1123)
```

#### **NOTE**

Press the **<Space>** bar to scroll down in the file.

4. Some of the `/export/home/sdc/nuevo/logfiles/network_scu_trace.log*` log files have wrong ownership (`root root` instead of `sdc sdc`). To check this type the command:

```
ls -la /export/home/sdc/nuevo/logfiles/network_scu_trace.log* <Enter>
```

the output can be something like this (can be fewer files, one or more with `root root` ownership):

```
-rw-r--r-- 1 sdc sdc 0 Feb 17 21:01 network_scu_trace.log
-rw-r--r-- 1 root root 0 Jan 22 14:25 network_scu_trace.log.1
-rw-rw-r-- 1 sdc sdc 0 Feb 18 19:57 network_scu_trace.log.1.lck
-rw-rw-r-- 1 sdc sdc 0 Feb 12 18:45 network_scu_trace.log.2
-rw-rw-r-- 1 sdc sdc 0 Feb 17 21:01 network_scu_trace.log.lck
```

**Solution:** To eliminate this issue change the /export/home/sdc/nuevo/logfiles/network\_scu\_trace.log\* files ownership and restart services:

1. Open the AW Server Console/terminal, login as **root**.
2. Change the /export/home/sdc/nuevo/logfiles/network\_scu\_trace.log\* files ownership:

```
chown sdc:sdc /export/home/sdc/nuevo/logfiles/network_scu_trace.log*
<Enter>
```

3. Make sure no one is connected and restart all services.

Refer to [3.4.1.8 Software Subsystem Restart on page 164](#).

4. To avoid reoccurrence of the issue (by automatically changing back the ownership of the files periodically in every 5 minutes):
  - a. Open the AW Server Console/terminal, login as **root**.
  - b. Open the cron table file:

```
crontab -e <Enter>
```

- c. The cron table file opens using "**vi**" editor. Go to the end of the file using the **<Down arrow>** key then press the **<o>** key to insert a line in the file.

- d. Copy/paste the below line to the end of the cron table file:

```
*/5 * * * * /usr/bin/chown sdc:sdc /export/home/sdc/nuevo/logfiles/
network_scu_trace.log*
```

#### NOTE

Copy the first line then append the second line (without blank space), as it should appear on one line in the file.

- e. Press **<Esc>** then **:wq** to save the file and exit.
- f. Verify the content is as intended in crontab configuration by typing

```
crontab -l <Enter>
```

The line added above should be present in the output of the command.

#### NOTE

This workaround may need to be reapplied, if the **Check DICOM** button is used when configuring a DICOM Host.

## 3.4.6.25 Licenses for applications not installing after an AW Server update or upgrade

**Problem:** During a software update or upgrade of a version prior to AWS3.2 Ext. 4.0 to a version AWS3.2 Ext. 4.0, the CoLA licenses file (/usr/share/FL\_Server/GemsLicense) is restored with wrong rights and ownership. This leads to inability to add new licenses, or remove/update existing licenses, to the CoLA server, and so to install the licenses for the applications.

The following types of error display at the floating license manager when licenses are added, updated, or removed:

The operation did not complete successfully. Please see the **Results** box below.

For licenses addition or update, the **Results** displays as:



For licenses removal, the **Results** displays as:



**Solution:** To eliminate this issue change the /usr/share/FL\_Server/GemsLicense file rights and ownership.

1. Open the AW Server Console/terminal, login as **root**.
2. Change the /usr/share/FL\_Server/GemsLicense file rights and ownership:

```
chmod 664 /usr/share/FL_Server/GemsLicense <Enter>
```

```
chown root:cola-server /usr/share/FL_Server/GemsLicense <Enter>
```

### 3.4.6.26 Backup/Restore compatibility issue with AW Server AET port number

**Problem:** During a software update or upgrade of a version prior to AWS3.2 Ext. 4.0 to a version AWS3.2 Ext. 4.0, the AW Server AET port number is not restored.

The following Plain AET / Port displays N/A in the Healthpage.

| System Configuration       |                                |
|----------------------------|--------------------------------|
| System ID                  | PL1600AW06                     |
| Platform version           | aws-3.2-4.0-4                  |
| Hostname / IP Address      | awsct02 / eth0: 172.16.126.189 |
| Encrypted (TLS) AET / Port | aws_CT02 / 2762                |
| Plain AET / Port           | aws_CT02 / N/A                 |

The following file restored from previous version is missing information:

```
/usr/share/gehc_security/eat/configs/integration.cfg
```

**Solution:** To eliminate this issue, after restore, some additional line(s) must be added to the /usr/share/gehc\_security/eat/configs/integration.cfg file:

1. Open the AW Server Console/terminal, login as **root**.

2. Backup the original file:

```
cd /usr/share/gehc_security/eat/configs <Enter>
```

```
cp integration.cfg integration.cfg.orig <Enter>
```

3. Add the following line(s) at the end of the integration.cfg file:

- a. Upgrade from Ext. 2.0, 3.0, 3.2 and 4.0:

```
echo "" >> integration.cfg <Enter>
```

```
echo "CONNECTION_TIMEOUT_VALUE=60000" >> integration.cfg <Enter>
```

- b. Upgrade from Ext. 1.2:

```
echo "" >> integration.cfg <Enter>
```

```
echo "AUDIT_SRC_ID_ENCODING_FORMAT=UTF-8" >> integration.cfg <Enter>
```

```
echo "MAX_AUDIT_SRC_ID_LENGTH=60" >> integration.cfg <Enter>
```

```
echo "DISABLE_TLS=false" >> integration.cfg <Enter>
echo "CONNECTION_TIMEOUT_VALUE=60000" >> integration.cfg <Enter>
```

4. Verify that the above line(s) are added to the `integration.cfg` file:

```
diff integration.cfg integration.cfg.orig <Enter>
```

The following line(s) are present in the result of the command:

- a. Upgrade from Ext. 2.0, 3.0, 3.2 and 4.0:

```
< CONNECTION_TIMEOUT_VALUE=60000
```

- b. Upgrade from Ext. 1.2:

```
< AUDIT_SRC_ID_ENCODING_FORMAT=UTF-8
```

```
< MAX_AUDIT_SRC_ID_LENGTH=60
```

```
< DISABLE_TLS=false
```

```
< CONNECTION_TIMEOUT_VALUE=60000
```

5. Restart all services. Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#).
6. Set the EAT configuration from the Service Tools.

### 3.4.6.27 DICOM transfer failure when DICOM Host Access Control change without system restart

**Problem:** When setting/changing the **DICOM Hosts Access Control** (from Service Tools under **Administrative > Configuration > DICOM Hosts** menu), the DICOM transfer fails (DICOM remote query (C-FIND SCU), copy to local (C-MOVE SCU) and send to (C-STORE SCU) services fail). This occurs because the services are not properly restarted after this setting, even if the message “Nuevo service restart completed.” popups.

**Solution:** To eliminate this issue, restart the services from the healthpage, as described in [3.4.1.8 Software Subsystem Restart on page 164](#).

#### NOTE

In certain cases services restart may not be sufficient. In this case, reboot the AW Server.

### 3.4.6.28 Cannot install the Edison Machine Light and Service outside the GE network

**Problem:** While installing the Enterprise Cockpit component, the Edison Machine Light and Service does not install. This is due to the Domain Name System (DNS) resolver which is wrongly configured and does not allow applications running in the operating system to translate human-friendly domain names into the numeric IP addresses that are required for access to resources on the local area network or the Internet.

**Solution:** To eliminate this issue, update the certificate management service helm chart. This update must be applied after Enterprise Cockpit components installation when the AW Server has finished to reboot:

1. Open the AW Server Console/terminal, login as **root**.
  2. Navigate to the `/export/home/eml_copy/helm` directory:
- ```
cd /export/home/eml_copy/helm <Enter>
```
3. Uncompress the certificate management service package:
- ```
tar -xf certificate-management-service-1.0.0-8b9903a.tgz <Enter>
```

4. Navigate to the certificate-management-service/templates directory:

```
cd certificate-management-service/templates <Enter>
```

5. Backup the flyway\_migration\_job.yaml file:

```
cp flyway_migration_job.yaml flyway_migration_job.yaml.orig <Enter>
```

6. Update the flyway\_migration\_job.yaml file:

```
sed -i 's/hc-eu-west.*jdk:0.17-alpine/"{{ .Values.initContainer.image }}:{{ .Values.initContainer.tag }}"/g' flyway_migration_job.yaml <Enter>
```

7. Verify that the flyway\_migration\_job.yaml file is updated correctly:

```
diff flyway_migration_job.yaml flyway_migration_job.yaml.orig <Enter>
```

The following lines appear twice:

```
< image: "{{ .Values.initContainer.image }}:
{{ .Values.initContainer.tag }}"
```

---

```
> image: hc-eu-west-aws-artifactory.cloud.health.ge.com/docker-eis-dev/
parth/flyway-jdk:0.17-alpine
```

8. Remove the flyway\_migration\_job.yaml.orig file:

```
rm flyway_migration_job.yaml.orig <Enter>
```

9. Navigate back to the /export/home/eml\_copy/helm directory:

```
cd /export/home/eml_copy/helm <Enter>
```

10. Package the certificate management service:

```
helm package certificate-management-service <Enter>
```

11. Remove the certificate management service file:

```
rm -fvr certificate-management-service <Enter>
```

### 3.4.6.29 Service/admin user login problems and/or log partition getting full causes system to get unavailable

**Problem:** On AWS3.2 Ext. 4.2 and Ext. 4.4, due to incorrectly set default password expiration rules, service/admin users may get locked out of Service Tools and cronjobs running under sdc user may not get executed, resulting in failure of logrotation. In extreme cases, the failure of logrotation can result in a completely filled logfile partition, making the system unavailable. The exact timing of the latter problem happening varies with system usage, but it is generally a few weeks, but possibly in a few days. If generic hardening is enabled after installation, service/admin passwords will expire in 60 days, with no easy way to change them.

#### NOTE

The execution of this workaround is mandatory on all **AW Server 3.2 Ext. 4.2 and Ext. 4.4** systems. In any case, the script can be reexecuted safely multiple times.

When the logrotation cronjobs are not executed and the disk gets full, the log disk space status becomes red in the Healthpage.

|                                |                                               |
|--------------------------------|-----------------------------------------------|
| Memory Total / Free            | 24576 (MB) / 18673 (MB)                       |
| OS Disk Space Total / Free     | 110 (GB) / 91 (GB)                            |
| Image Disk Space Total / Free  | 291 (GB) / 235 (GB)                           |
| Backup Disk Space Total / Free | 3 (GB) / 3 (GB)                               |
| Log Disk Space Total / Free    | 19 (GB) / 0 (GB)                              |
| Network Queue Status           | In progress: 0 Pending: 0 Paused: 0 Failed: 0 |

If the service/admin password is expired, the following error message will apply:

- AW Server 3.2 Ext. 4.2:



- AW Server 3.2 Ext. 4.4:



**Solution:** To prevent the problems to occur and to solve the problems when it already occurred, execute the below attached script in the AW Server.

#### NOTE

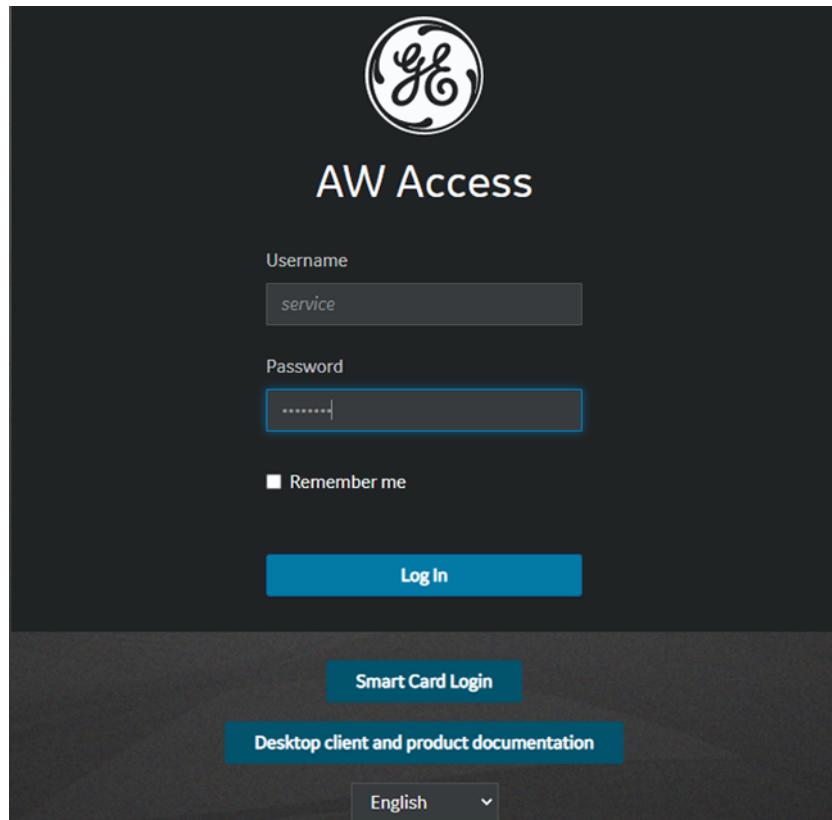
In the below steps, it is ask to transfer the attached script into the AW Server. If the system is remotely connected through RSvP (either the AW Server itself, or the NanoCloud/Edison HealthLink), then perform the file transfer at FFA.

1. Copy the `fix-sdc-expired.sh` file on the PC:
  - a. Right-click here\_\_\_\_\_, and using the contextual menu that displays, copy the file on the PC.

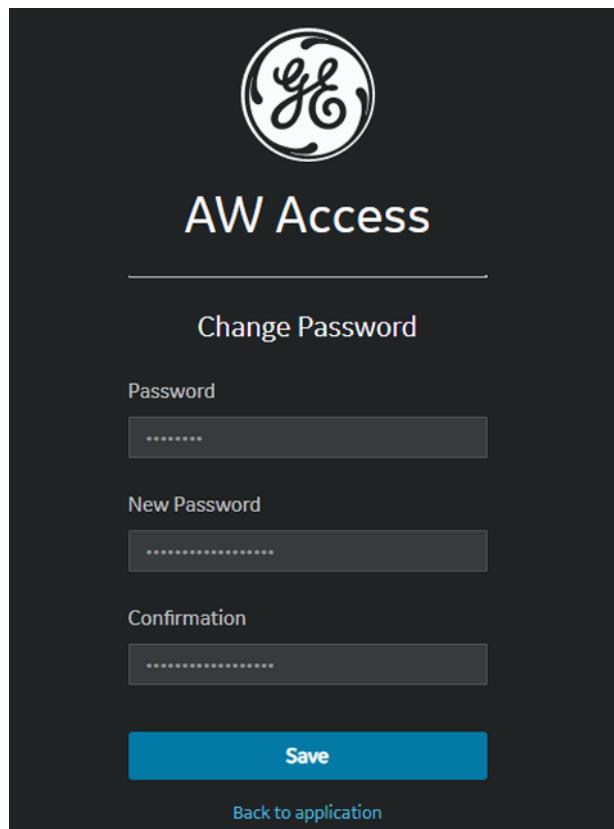
#### NOTE

To view and open a pdf attachment, the pdf must be opened with Acrobat® Reader® X or later version. To be able to download the attached file, an upgrade of Acrobat® Reader® to a newer version may be needed.

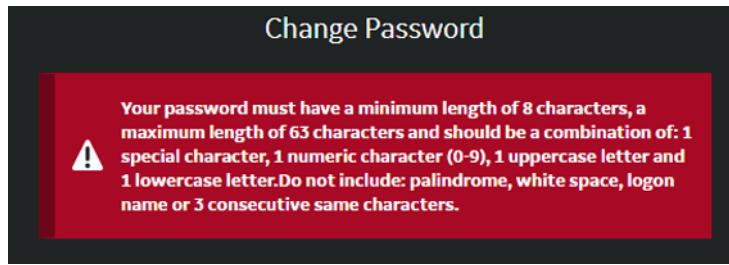
2. On Virtual or Physical AW Server:
  - a. Launch the AW Server Service Tools on the PC, and login as **service**.
  - b. If the **service** password has expired, renew it:
    - i. Open a Web Browser on the PC and type in:  
**https://<AW Server IP address>/auth/realm/aws/account/password**
    - ii. In the login screen, enter the service user and the current **service** password.



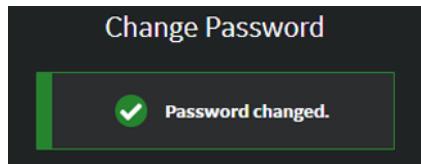
- iii. In the change password screen, set the current password, the new password, confirm it and click on **Save**.



- iv. If the new password does not follow the rules and guidelines, the following message displays:



- v. If the password change is successful, the following message displays:



#### **NOTE**

In some cases, this message may not appear, only the password fields get emptied without any error message appearing. The new password should still work.

3. On NanoCloud:
  - a. Launch the AW Server Service Tools.  
On the CT Console, start the Service Desktop interface using the CSD tool and select **Configuration > Configuration AWS on VM > Launch AWS Service Tools**.
  - b. If the **service** password has expired, renew it:
    - i. Open a Web Browser on the CT Console and type in:  
**https://192.168.101.5/auth/realm/aws/account/password**
    - ii. Renew the password as described in [Step 2.b](#) from the second point.
  - c. Copy the **fix-sdc-expired.sh** file into an USB key.
  - d. Insert the USB key into the CT Console.
  - e. Open a console/terminal on the CT Console.
  - f. Mount the USB partition by typing following command in the console/terminal:  
**mountUSB <Enter>**

#### **NOTE**

Ignore the message that displays when mounting the USB key.

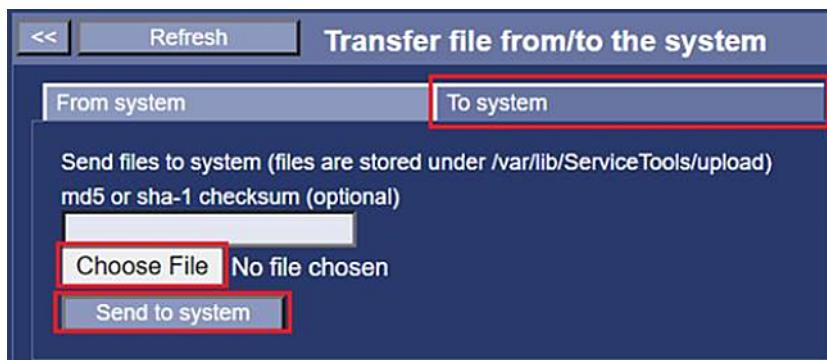
- g. Copy the **fix-sdc-expired.sh** file on the CT Console:  
**cp /USB/fix-sdc-expired.sh /usr/g/ctuser/Downloads <Enter>**
- h. Unmount the USB partition and remove the USB key from the CT Console:  
**umountUSB <Enter>**

4. On Edison HealthLink:
  - a. Launch the AW Server Service Tools.

Open a Web Browser on the PC and type in:

**https://<Edison Private proxy floating IP address>:5443**

- b. If the **service** password has expired, renew it:
  - i. Open a new tab in the Web Browser and type in:  
**https://<Edison Private proxy floating IP address>:5443/auth/realm/aws/account/password**
  - ii. Renew the password as described in [Step 2.b](#) from the second point.
5. Upload the `fix-sdc-expired.sh` file into the AW Server:
  - a. From the Service Tools, select **Tools > File Transfer**.
  - b. In the **To System** tab, click on **Choose File** and select the `fix-sdc-expired.sh` file stored on the PC (or on the CT Console or the EHL system).



- c. To upload the `fix-sdc-expired.sh` file click on **Send to system**.

**NOTE**

The `fix-sdc-expired.sh` file is uploaded into the `/var/lib/ServiceTools/upload` location.

- d. When the file is loaded, click on **OK** in the pop-up window.
  6. Open or display the AW Server Console/terminal, login as `root`.
  7. In the AW Server Console/terminal, copy the `fix-sdc-expired.sh` file, previously uploaded, in the `/tmp` directory:
- ```
cp /var/lib/ServiceTools/upload/fix-sdc-expired.sh /tmp <Enter>
```
8. Execute the `fix-sdc-expired.sh` script:
- ```
sh /tmp/fix-sdc-expired.sh <Enter>
```

The output of the command displays the new **sdc** password. Please note it to remember it.

```
[root@bucaw70-239 ~]# sh /tmp/fix-sdc-expired.sh
Messages are logged to /var/log/gehc/fix-sdc-expired.log
Checking if log partition is under 80% <-> 5: OK
Deactivating password hardening for sdc user
Changing password for user sdc.
passwd: all authentication tokens updated successfully.
Deactivating password hardening for sdc user
Verifying sdc password never expires : : OK
Verifying sdc password is active : : OK
Verifying sdc password must not be changed : : OK
Executing EA3 hardening for MMSR
 with STIG: V-69555: OK
 with STIG: V-69557: OK
 with STIG: V-69571: OK
 with STIG: V-69573: OK
 with STIG: V-69575: OK
 with STIG: V-69577: OK
Changing password expiration for admin/service users to 1024 days: OK
Password for "service" will expire in 954 days: No change required
WARNING: Password for "sdc" user has been renewed to "OWFiZDNjN2VkMDk0=", please note it!
```

### 3.4.6.30 AW Server on CT Nano-Cloud does not start after CT Console reboot

**Problem:** AW Server on CT Nano-Cloud does not start after a CT Console reboot. This occurs because the *nuevo* service startup sequence times out.

**Solution:** To eliminate this issue, increase the timeout period of the *nuevo* service startup sequence.

1. Open the AW Server Console/terminal, login as **root**.
2. Navigate to the *nuevo* startup directory:

```
cd /export/home/sdc/nuevo/scripts/startup <Enter>
```

3. Backup the *nuevo* service script:

```
cp nusmd nusmd.orig <Enter>
```

4. Update the timeout period of the *nuevo* service script:

```
sed -i 's/^noRetries = .*$/noRetries = 30/g' nusmd <Enter>
```

```
sed -i 's/^timeOut = .*$/timeOut = 2/g' nusmd <Enter>
```

5. Verify that the *nuevo* service script is updated correctly:

```
diff nusmd nusmd.orig <Enter>
```

The following lines appear:

```
< noRetries = 30
< timeOut = 2

> noRetries = 10
> timeOut = 1
```

6. Restart all services. Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#).

### 3.4.6.31 Service restart and data loading problems

**Problem:** On AWS3.2 Ext. 4.6 due to timeout issues, the AW Server services fail to start after Software Subsystem / Restart command executed by the Service or Admin user from Service Tools. Also for similar reasons application users can experience problems with loading data.

#### NOTE

The execution of this workaround is mandatory on all **AW Server 3.2 Ext. 4.6** systems right after installation. In any case, the script can be re-executed safely multiple times also later.

**Solution:** To prevent the problems to occur and to solve the problems when it already occurred, execute the below attached script in the AW Server.

#### NOTE

In the below steps, it is asked to transfer the attached script into the AW Server. If the system is remotely connected through RSvP (either the AW Server itself, or the NanoCloud/Edison HealthLink), then perform the file transfer at FFA.

1. Copy the `fix-ext46-01.sh` file **embedded into this pdf document**:

- Right-click here\_\_\_\_\_, and using the contextual menu that displays, copy the file on the PC.

**NOTE**

To view and open a pdf attachment, the pdf must be opened with Acrobat® Reader® X or later version. To be able to download the attached file, an upgrade of Acrobat® Reader® to a newer version may be needed.

- On NanoCloud, copy the `fix-ext46-01.sh` file into the CT Console:
  - Copy the `fix-ext46-01.sh` file into an USB key.
  - Insert the USB key into the CT Console.
  - Open a console/terminal on the CT Console.
  - Mount the USB partition by typing following command in the console/terminal:

`mountUSB <Enter>`

**NOTE**

Ignore the message that displays when mounting the USB key.

- Copy the `fix-ext46-01.sh` file on the CT Console:

`cp /USB/fix-ext46-01.sh /usr/g/ctuser/Downloads <Enter>`

- Unmount the USB partition and remove the USB key from the CT Console:

`umountUSB <Enter>`

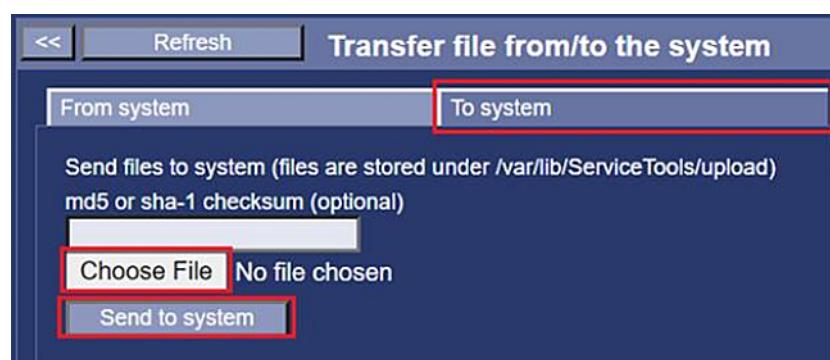
- Upload the `fix-ext46-01.sh` file into the AW Server:

- Launch the AW Server Service Tools, and login as **service**:

- On Virtual or Physical AW Server, open a Web Browser on the PC and type in the AW Server IP address.
- On Edison HealthLink, open a Web Browser on the PC and type in:  
`https://<Edison Private proxy floating IP address>:5443`
- On NanoCloud, on the CT Console, start the Service Desktop interface using the CSD tool and select **Configuration** > **Configuration AWS on VM** > **Launch AWS Service Tools**.

- Upload the `fix-ext46-01.sh` file into the AW Server:

- From the Service Tools, select **Tools** > **File Transfer**.
- In the **To System** tab, click on **Choose File** and select the `fix-ext46-01.sh` file stored on the PC (or on the CT Console or the EHL system).



- To upload the `fix-ext46-01.sh` file click on **Send to system**.

**NOTE**

The fix-ext46-01.sh file is uploaded into the /var/lib/ServiceTools/upload location.

- iv. When the file is loaded, click on **OK** in the pop-up window.
3. Execute the workaround script fix-ext46-01.sh:
- a. If the system is not in Maintenance mode already, then put the AW Server in Maintenance mode, because the script will cause the services to restart which will break all ongoing user sessions.
  - b. Open or display the AW Server Console/terminal, login as **root**.
  - c. In the AW Server Console/terminal, copy the fix-ext46-01.sh file, previously uploaded, in the /tmp directory:
- ```
cp /var/lib/ServiceTools/upload/fix-ext46-01.sh /tmp <Enter>
```
- d. Execute the fix-ext46-01.sh script:
- ```
sh /tmp/fix-ext46-01.sh <Enter>
```

The output of the command displays the following:

- On NanoCloud and Edison Healthlink:

```
Messages are logged to /var/log/gehc/fix-ext46-01.log
Tue May 31 13:10:07 CEST 2022 Fixing processDefaultTimeoutMs...
Tue May 31 13:10:07 CEST 2022 Fixing pacsinteg timeouts...
Tue May 31 13:10:07 CEST 2022 PACSPlugin timeout patch not found,
applying ...
Tue May 31 13:10:07 CEST 2022 PACSPlugin timeout applyied,
restarting aweservice ...
Tue May 31 13:10:12 CEST 2022 PACSPlugin timeout patch not found
in pacsinteg-webservice, applying ...
Tue May 31 13:10:12 CEST 2022 PACSPlugin timeout applyied,
restarting pacsinteg-webservice ...
```

- On Standalone AW Server:

```
Messages are logged to /var/log/gehc/fix-ext46-01.log
Tue May 31 13:14:21 CEST 2022 Fixing processDefaultTimeoutMs...
Tue May 31 13:14:21 CEST 2022 Pacsinteg webservice is not
running, no need to fix!
```

- e. Finish Maintenance mode.

### 3.4.6.32 Application Usage Monitor not working in NanoCloud AW Server

**Problem:** The Application Usage Monitor (software-metering component) is not working in NanoCloud AW Server. This issue occurs when AW Server installation is completed and after the reboot.

**Detection:** To check that the issue faced is the one described above, follow the below procedure:

1. Open the AW Server Console/terminal, login as **sdc**.
2. Display the list of database:

```
psql -d postgres -l <Enter>
```

The output of the command should be as:

| List of databases |       |          |             |             |                   |   |
|-------------------|-------|----------|-------------|-------------|-------------------|---|
| Name              | Owner | Encoding | Collate     | Ctype       | Access privileges |   |
| dbexpress         | sdc   | UTF8     | en_US.UTF-8 | en_US.UTF-8 |                   |   |
| postgres          | sdc   | UTF8     | en_US.UTF-8 | en_US.UTF-8 |                   |   |
| swmetering        | astp  | UTF8     | en_US.UTF-8 | en_US.UTF-8 | astp=CTc/astp     |   |
| template0         | sdc   | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/sdc            | + |
|                   |       |          |             |             | sdc=CTc/sdc       |   |
| template1         | sdc   | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/sdc            | + |
|                   |       |          |             |             | sdc=CTc/sdc       |   |

(5 rows)

- If the swmetering row, highlighted in red in the above screen capture, is not displayed, then the issue is present.

Follow the below steps to eliminate the issue.

**Solution:** To eliminate this issue, execute the swmetering installation script:

- In the AW Server Console/terminal, change user to **root** and enter the **root** password.

```
su - <Enter>
```

- Execute the swmetering installation script:

```
/export/home/sdc/swmetering/dbfiles/scripts/install_swm_schema.sh
<Enter>
```

- In the AW Server Console/terminal, change user to **sdc**.

```
su - sdc <Enter>
```

- Display the list of database:

```
psql -d postgres -l <Enter>
```

The output of the command should display the swmetering row, as in the screen capture above.

### 3.4.6.33 Cannot mount USB media on Nano-Cloud

**Problem:** On Nano-Cloud, the USB media cannot be mounted. This issue occurs when the USB media is created with AWeDIM tool and mounted using the **mountUSB** command. Indeed, the AWeDIM tool creates two partitions in the USB media, one in FAT32 which is bootable for the OS (not used here) and the second in NTFS which actually contains the iso/package file. However, the **mountUSB** command can mount only the FAT32 partition.

**Solution:** To eliminate this issue, mount the USB media as followed:

- Insert the USB media into the CT Console.

- Open a Console/terminal on the CT Console, login as **root**.

- Mount the USB partition by typing:

```
mount /dev/disk/by-label/AW_DATA /mnt <Enter>
```

- Copy the iso/package file into the `/usr/g/AWS_VM` directory and change the rights to **ctuser**:

```
cp /mnt/<iso or package> /usr/g/AWS_VM <Enter>
```

```
chown ctuser:ctuser /usr/g/<iso or package> <Enter>
```

#### NOTE

Replace `<iso or package>` file by the actual name on the USB media. For instance:

`VV_Apps_16.0ext4._sw_aw_aws.iso`.

5. Unmount the USB partition and remove the USB media from the CT Console:

```
umount /mnt <Enter>
```

### 3.4.6.34 Database corruption in Nano-Cloud AW Server

**Problem:** In Nano-Cloud AW Server, when saving images in Volume Viewer, the images cannot be recorded in the database. This issue is due to a database corruption, and in this case, the following message is displayed Declaration in database failed.

**Solution:** To eliminate this issue, rebuild the database as follow:

1. If the system is not in Maintenance mode already, then put the AW Server in Maintenance mode.
2. Open the AW Server Console/terminal, login as **sdc**.
3. Rebuild the database by typing the following commands:

```
nusm stop <Enter>
```

```
sdc_database.sh build <Enter>
```

4. Restart all services. Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#).
5. Finish Maintenance mode.
6. Check that images can be saved when using Volume Viewer in the CT Console.

### 3.4.6.35 Filmer export to PDF function does not work

**Problem:** The Filmer export to PDF function is broken. This occurs on the AW Server 3.2 Ext. 4.0 and up when restoring the configuration from a backup of an AW Server 3.2 Ext. 3.2 or earlier releases. In this case an obsolete /export/home/sdc/Prefs/DataExport file is restored and it breaks the Filmer export to PDF function.

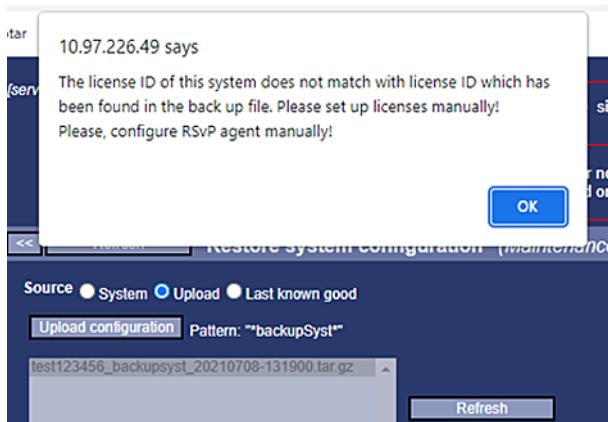
**Solution:** To eliminate the issue, remove the /export/home/sdc/Prefs/DataExport file (this file will be recreated by the Filmer with the correct content the first time the export to PDF feature will be used):

1. Open the AW Server Console/terminal, login as **sdc**.
2. Remove the /export/home/sdc/Prefs/DataExport file:

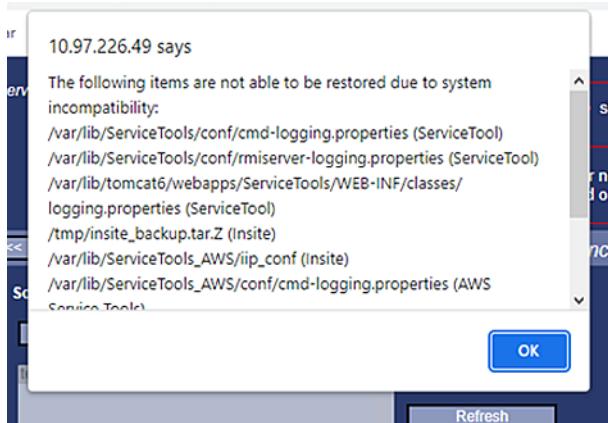
```
rm -rf /export/home/sdc/Prefs/DataExport <Enter>
```

### 3.4.6.36 EA3 component corruption after system configuration restoration failure

**Problem:** While restoring a full system configuration backup of a version prior to AW Server 3.2 Ext. 4.2 into an AW Server 3.2 Ext. 4.2 or up, if the restoration fails, the EA3 component get corrupted. This occurs while the licensing restoration component is problematic (like licenseID changed due to MAC address change or to OS change). In this case the following popup displays when the backup file is selected:



The following popup might also appear:



If this happens and the warning are ignored, and the full restoration is done, the licensing part fails and the EA3 component gets corrupted. Then the Service Tools login will fail (**Do not logout the Service Tools now**) and a Load From Cold will be required.

**Detection:** To check that the issue faced is the one described above, perform the following steps:

1. Open the AW Server Console/terminal, login as **root**.
2. List the content of the ea3 directory:

```
ls $GEHC_SECURITY_HOME/ea3 <Enter>
[root@bucaw70-237 ~]# ls $GEHC_SECURITY_HOME/ea3
configs ea3ShData.1 inactivity integration licenses scripts userdb
ea3Share images inactivity64 jar logs ssa version.txt
```

The ea3 directory contains 12 directories (in blue in the output of the command above). If less directories are present, then the issue is present.

**Solution:** To eliminate the issue and prevent a Load From Cold, recover the EA3 component and restore the other components separately:

1. The EA3 component has been moved to the /tmp/ea3\_native.tgz file, due to the restoration failure.

#### NOTE

**Do not reboot** the AW Server before moving the EA3 component back to the right location. Otherwise the /tmp directory will be emptied and the EA3 component could not be recovered. Which will lead to the need to perform a Load From Cold.

2. Navigate to the gehc\_security directory:

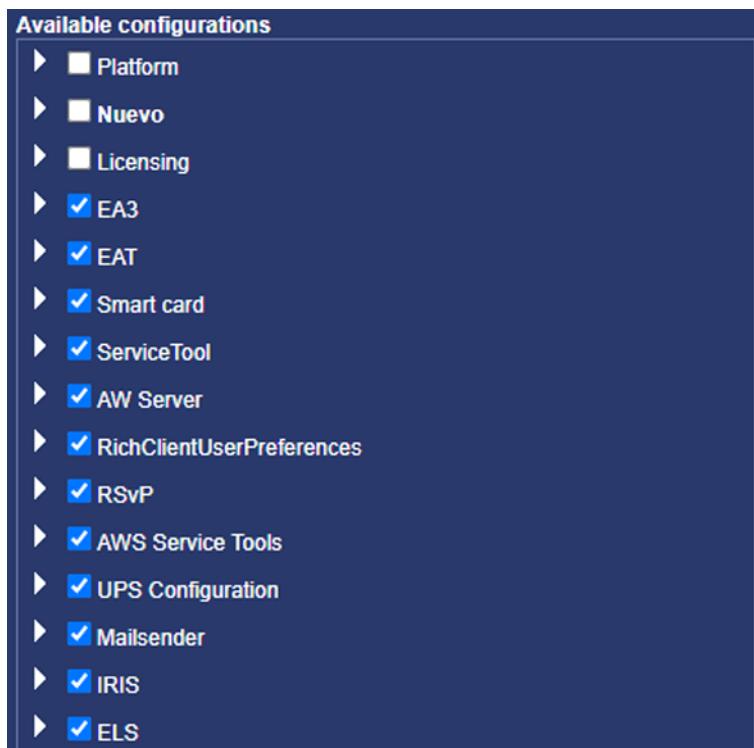
```
cd $GEHC_SECURITY_HOME <Enter>
```

3. Copy the EA3 files back to the right location:

```
tar xf /tmp/ea3_native.tgz <Enter>
```

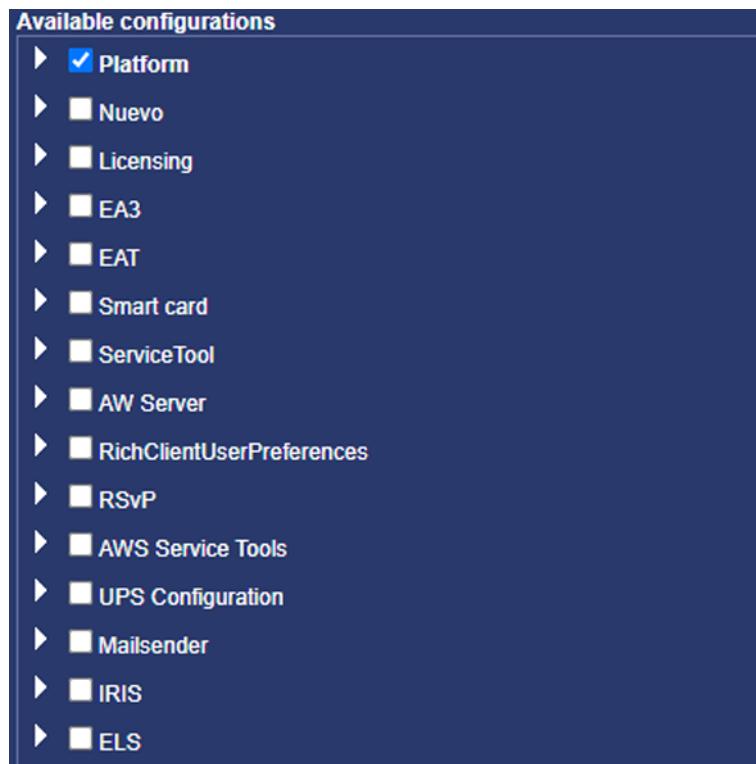
4. Check that it is possible to login into the Service Tools:
  - a. Logout the Service Tools.
  - b. Login again as usual into the Service Tools.
5. Reboot the AW Server to recover the **Maintenance > Restore > System configuration** page of the Service Tools:

From the Service Tools , select **Tools > Reboot**, then click on **Reboot AW Server**.
6. Once rebooted (once you can login again into the Service Tools), restore the same backup file with unselecting all components in the content list before **EA3** checkbox.
  - a. From the Service Tools, select **Maintenance > Restore > System configuration**, select the backup file.
  - b. Uncheck the components before **EA3** checkbox.



- c. Click **Restore Selected**.
7. Restore all components in the content list before **EA3** checkbox, **one by one except Licensing** component.

- Uncheck all the components and check one component before **EA3** checkbox.



- Click **Restore Selected**.
- Repeat the above steps, for the other component before **EA3** checkbox.

#### **Important**

Do NOT restore **Licensing** NOR **EA3** components.

- If the issue is still present, perform a Load From Cold.

### 3.4.6.37 Platform analytics sweep scripts cannot get application usage information from sites

**Problem:** The platform analytics sweep scripts cannot get application usage information from sites and therefore cannot get any usage information that they are using further. The whole software-metering component was put behind realm-authentication, which causes issue.

**Solution:** To eliminate this issue, update the *swmetering* xml script:

- Open the AW Server Console/terminal, login as **root**.
- Navigate to the *swmetering* xml scripts directory:

```
cd /var/lib/tomcat/webapps/swmetering/WEB-INF <Enter>
```

- Backup the *swmetering* xml script:

```
cp web.xml web.xml.orig <Enter>
```

- Open the *web.xml* file, using **vi** editor:

```
vi web.xml <Enter>
```

- Navigate in the file using the **<arrow>** keys, and move the cursor till **just before the line </web-app>** at the end of the file.

- Press the **<o>** key to insert a line below the cursor (so just before the line *</web-app>*).

- Add (copy/paste) the following lines:

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Public</web-resource-name>
<description>Enable usage data fetching without authentication.</description>
<url-pattern>/getData.fetch</url-pattern>
</web-resource-collection>
</security-constraint>
```

- Press **<Esc>** to exit the editor mode.
- To save the file and exit type **:wq** then press **<Enter>**.
- Verify that the **web.xml** file is updated correctly:

```
diff web.xml web.xml.orig <Enter>
```

The following lines appear:

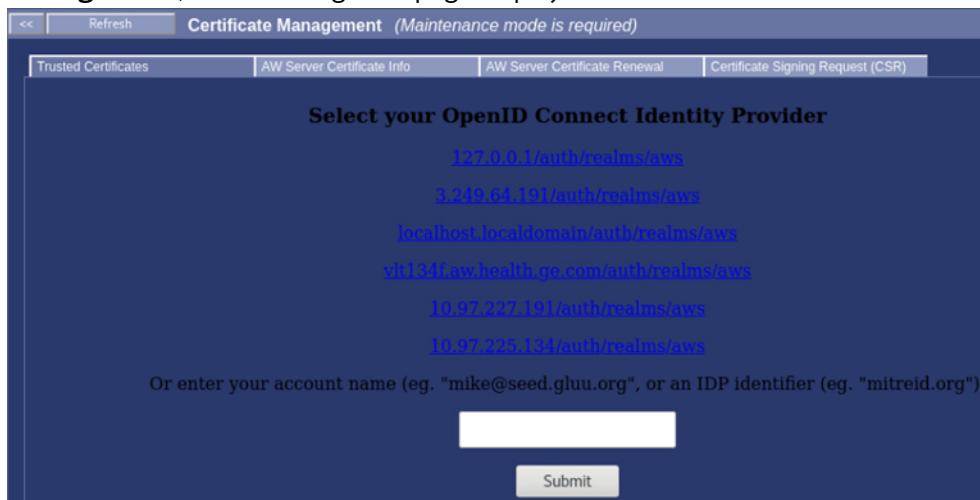
```
< <security-constraint>
< <web-resource-collection>
< <web-resource-name>Public</web-resource-name>
< <description>Enable usage data fetching without authentication.</
description>
< <url-pattern>/getData.fetch</url-pattern>
< </web-resource-collection>
< </security-constraint>
```

This should take effect after few seconds (~ 10 sec).

### 3.4.6.38 Login panel is not displayed in Certificate Management page

**Problem:** The Certificate Management page does not display the login panel. This occurs when attempting to launch the Service Tools remotely (e.g.: From FFA or from the KVM locally (on a physical HW) or (on virtual environment) using "**Launch web console**" (with the **startx** command)).

In this case, from the Service Tools, in **Administrative > Configuration > Certificate Management**, the following such page displays:



**Solution:** To eliminate this issue, either try to use one of the links displayed in the wrong page above, or follow the below steps:

- Get the IP address (or the FQDN name) displayed in the URL field of the navigator, while starting the Service Tools.

For instance:



Or from FFA, with the port number (in case of CSD VNC service tool, as in the example below) or without port number (in case of HTTPS connectivity tool):



- Open the AW Server Console/terminal, login as **root**.
- Navigate to the /opt/keycloak/bin directory:

```
cd /opt/keycloak/bin <Enter>
```

- Launch the following command with the IP address or FQDN (Fully Qualified Domain Name) of the Service Tools and port number if needed:

```
python3 set_multiple_host_config.py <IP/FQDN, with ports for FFA>
<Enter>
```

For instance:

```
python3 set_multiple_host_config.py localhost <Enter>
```

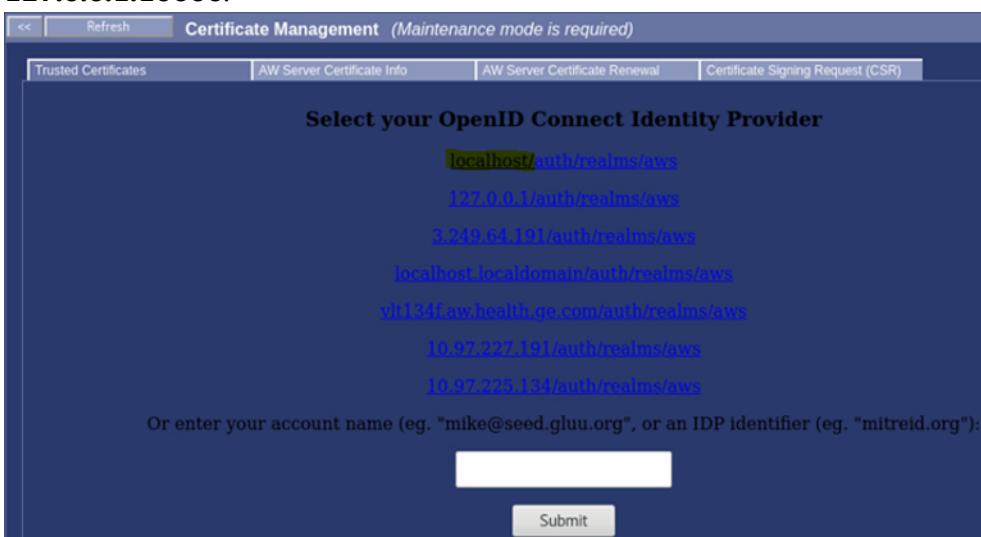
Or from FFA, with the port number (assuming that the port number is 10000):

```
python3 set_multiple_host_config.py 127.0.0.1:10000 <Enter>
```

- Click on **Refresh** button to refresh the Certificate Management page in the Service tools.

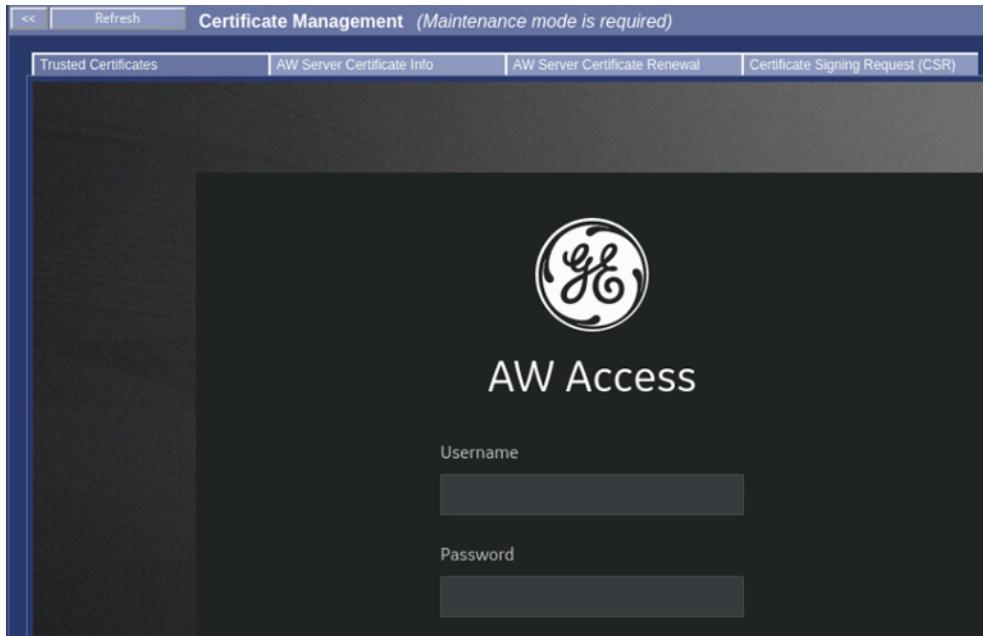
The Certificate Management page displays with a new link related to the command launched in [Step 4](#):

In the example below, the first command example in [Step 4](#) has been launched, so the new link starts with **localhost**. For the second command example the new link would start with **127.0.0.1:10000**.



- Select the new link in the page above.

The login panel displays in the Certificate Management page:



### 3.4.6.39 3D application not starting after restoring backup containing Web Client settings

**Problem:** On AW Servers with Web Client installed, after restoring a backup file that includes settings for Web Client and Imaging Fabric based (Web Client only) applications, the 3D applications do not start. This occurs because the log files in `/var/log/gehc/fluentlogs` start to indefinitely grow in size (multiple MB/minute), which leads to the log file partition getting full.

**Solution:** To eliminate this issue, follow the below steps:

1. Open the AW Server Console/terminal, login as **root**.
2. Run the following command:

```
kubectl exec $(kubectl get pods -A | grep 'eis-common-postgres-postgresql.*Running' | awk '{print $2}') -n edison-system -- psql -U ccs -d ccs_db -c "delete from config_audit; update config_data set revision=1" <Enter>
```

### 3.4.6.40 Cannot load Save State created by AW Server applications in Micro Cloud (AW Server hosted by Edison HealthLink)

**Problem:** In Micro Cloud (AW Server hosted by Edison HealthLink (EHL)), the Save State created by AW Server applications cannot be loaded. When the Save State is created, using an AW Server application (Volume Viewer, Reformat, ...), the user cannot later access and load the Save State and the AW Server displays an error message.

**Solution:** To eliminate this issue, update the `aweservice` and `pacsinteg-webservice.service` files:

1. Open the AW Server Console/terminal, login as **root**.
2. Navigate to the `/etc` directory:

```
cd /etc <Enter>
```

3. Backup the `aweservice` file:

```
cp aweservice aweservice.orig <Enter>
```

4. Update the `aweservice` file:

```
sed -i "s/\\(QIDO_OPTIMIZATION '\\)true/\\1false/" aweservice <Enter>
```

5. Verify that the aweservice file is updated correctly:

```
diff aweservice aweservice.orig <Enter>
```

The following lines appear (check the change in bold):

```
< /usr/bin/su - $AWE_USER -c "setenv JAVA_TOOL_OPTIONS '-
Dsun.java2d.xrender=false'; setenv QIDO_OPTIMIZATION 'false';
setenv QIDO_OPTIMIZATION_EXCLUDED_IMAGE_TYPES 'VXTL STATE'; setenv
QIDO_OPTIMIZATION_EXCLUDED_MODALITIES 'PR:RTIMAGE:RPLAN:RTSTRUCT' ;$AWE_BIN
$VERBOSE" 0<&- 1>/dev/null 2>&1 &

> /usr/bin/su - $AWE_USER -c "setenv JAVA_TOOL_OPTIONS '-Dsun.java2d.xrender=false'; setenv
QIDO_OPTIMIZATION 'true'; setenv QIDO_OPTIMIZATION_EXCLUDED_IMAGE_TYPES 'VXTL
STATE'; setenv QIDO_OPTIMIZATION_EXCLUDED_MODALITIES 'PR:RTIMAGE:RPLAN:RTSTRUCT' ;
$AWE_BIN $VERBOSE" 0<&- 1>/dev/null 2>&1 &
```

6. Restart the aweservice service:

```
systemctl restart aweservice <Enter>
```

7. Navigate to the /usr/lib/systemd/system directory:

```
cd /usr/lib/systemd/system <Enter>
```

8. Backup the pacsinteg-webservice.service file:

```
cp pacsinteg-webservice.service pacsinteg-webservice.service.orig
<Enter>
```

9. Update the pacsinteg-webservice.service file:

```
sed -i 's/^(QIDO_OPTIMIZATION=)true/\1false/' \
pacsinteg-webservice.service <Enter>
```

10. Verify that the pacsinteg-webservice.service file is updated correctly:

```
diff pacsinteg-webservice.service pacsinteg-webservice.service.orig
<Enter>
```

The following lines appear:

```
< Environment=QIDO_OPTIMIZATION=false
```

```

```

```
> Environment=QIDO_OPTIMIZATION=true
```

11. Reload systemctl daemon:

```
systemctl daemon-reload <Enter>
```

12. Restart the pacsinteg-webservice service:

```
systemctl restart pacsinteg-webservice <Enter>
```

### 3.4.6.41 Cannot open 2D datasets on AW Enterprise systems

**Problem:** AW Enterprise does not currently have means to view 2D datasets (e.g. X-rays, CT scout images, RT dose reports) since Volume Viewer cannot open these datasets and 2D Viewer is disabled due to performance constraints.

**Solution:** Since 2D Viewer is fully functional in AW Enterprise systems apart from the performance issues, it can be reenabled by changing the following two property files:

1. Open the AW Server Console/terminal, login as **root**.

2. Navigate to the /export/home/sdc/server/prefs/ directory:

```
cd /export/home/sdc/server/prefs/ <Enter>
```

3. Backup the ServerPreferences.properties file:

```
cp ServerPreferences.properties ServerPreferences.properties.orig
<Enter>
```

4. Update the ServerPreferences.properties file:

```
sed -i 's#viewerManager/integration/hybrid#viewerManager/integration/full#' ServerPreferences.properties <Enter>
```

5. Verify that the ServerPreferences.properties file is updated correctly:

```
diff ServerPreferences.properties ServerPreferences.properties.orig
<Enter>
```

The following lines appear (check the changes in bold):

```
</com/ge/med/awe/app/nxapp/launchAtLogon/viewerManager/integration/full
```

---

```
>/com/ge/med/awe/app/nxapp/launchAtLogon/viewerManager/integration/hybrid
```

6. Navigate to the /export/home/sdc/client/prefs/ directory:

```
cd /export/home/sdc/client/prefs/ <Enter>
```

7. Backup the CommonPreferences.properties file:

```
cp CommonPreferences.properties CommonPreferences.properties.orig
<Enter>
```

8. Update the CommonPreferences.properties file:

```
sed -i 's#2DViewer/integration/hybrid#2DViewer/integration/full#' \
CommonPreferences.properties <Enter>
```

9. Verify that the CommonPreferences.properties file is updated correctly:

```
diff CommonPreferences.properties CommonPreferences.properties.orig
<Enter>
```

The following lines appear (check the changes in bold):

```
<<entry key="/com.ge.med.solo.process/actions/2DViewer/integration/full">
```

---

```
><entry key="/com.ge.med.solo.process/actions/2DViewer/integration/hybrid">
```

10. Restart the aweservice service:

```
systemctl restart aweservice <Enter>
```

#### NOTE

2D Viewer in AW Enterprise only provides acceptable performance for 2D datasets containing up to 10 images. Any dataset larger than that may take a very long time to load. Please advise the customer to always select the exact series they would like to open in 2D Viewer, instead of selecting the whole study.

## 3.4.7 Troubleshooting applications and licenses

Applicability*	AW Server 3.2 Extension											
	1.0	1.2	2.0	3.0	3.2	3.4	4.0	4.2	4.4	4.6	4.8	4.9
3.4.7.1 Uninstall Node-Locked Licenses on page 259	X	X	X	X	X	X	X	X	X	X	X	X
3.4.7.2 No licenses displayed in Floating License Manager on page 260	X	X	X	X	X	X	X	X	X	X	X	X
3.4.7.3 CardIQ Xpress Process does not generate series on page 261	X	X	X	X	X	X	X	X	X	X	X	X
3.4.7.4 2D Viewer does not launch on page 261	X	X	X									
3.4.7.5 System could not supply enough resources for Volume Viewer on page 262					X							
3.4.7.6 Graphic performance degraded when paging in Volume Viewer on page 262	X	X	X	X	X	X	X	X	X	X	X	X
3.4.7.7 Applications interactive performance degradation on page 263	X	X	X	X	X	X						
3.4.7.8 Dotmed communication causes AW Server performance degradation when loading many volumes in Volume Viewer on page 264						X	X	X				
3.4.7.9 Cannot launch applications in Hybrid integration mode with the PACS 3rd party integrated AW Server Client on page 265						X	X					
3.4.7.10 Logging-out from AW Server Client causes AW Server performance degradation on page 266							X					
3.4.7.11 Some Volume Viewer shortcuts are executed twice when Volume Viewer is started with Web Access on page 267								X	X	X	X	
3.4.7.12 SmartScore custom templates are not saved correctly on page 268							X					
3.4.7.13 Scrolling is slow and choppy in Volume Viewer viewport within Universal Viewer on page 269	X	X	X	X	X	X	X	X	X	X	X	X

\*An empty cell means the problem is not present or has been fixed in the corresponding extension.

### NOTE

In the below workarounds when a file is updated, it is requested to backup it (copy the file into <filename>.orig – the extension may differ). So, if some mistakes occur while executing the workarounds, it is recommended to recover the backup file (copy the backup file into the original file) and to re-execute the workaround.

## 3.4.7.1 Uninstall Node-Locked Licenses

### 3.4.7.1.1 Issue

If you install inadvertently NL (Node-locked) application licenses, they will not be listed by the Floating License Manager in the Service Tools. Nor can you replace them with Floating licenses without first deleting the NL licenses.

### 3.4.7.1.2 Workaround

1. If appropriate, convert each Node-locked license to Floating in the customer order (needs OCCR - this may change in the near future).

2. Login to the server through SSH (you may need to first enable ssh with ssh\_enabler through the Terminal Tool of ServiceTools).
3. List installed licenses by entering the following command in a Terminal window on the server:  
**licenseAdmin -slist <Enter>**
4. Delete Node-locked licenses from the server by entering the following commands in the Terminal window:  
**su - gehc\_security <Enter>**  
**licenseAdmin -delete <licenseName> <Enter>**  
**exit <Enter>**
5. Install the replacement Floating license(s) using the Floating License Manager in the Service Tools (**Administrative menu > Configuration > Floating License**) -

The Floating licenses will now be correctly installed and listed.

## 3.4.7.2 No licenses displayed in Floating License Manager

### 3.4.7.2.1 Issue #1

In the Service Tools, in **Initial Configuration > Licensing > Floating License**, no licenses are displayed even though the Floating License Server has been configured.

"License ID", "Name/IP", "Version" and "License Info" display as "N/A". The IP address is correctly displayed.

In **Diagnostic > Floating License**, no licenses are displayed. Hostname, License ID, Version display errors. The IP address is correctly displayed.

### 3.4.7.2.2 Solution issue #1

In **Initial Configuration > Licensing > CoLA Server**, check the 2 following things:

- Check that the IP address you entered for Primary License Server is correct. You can use the "Check Server IP" button to ping the corresponding IP address. Be aware that this test does only a simple ping to the IP address, so it does not ensure that the IP address corresponds to a Floating License server.
- Check that the Server Port is correct. By default, the port is 17767, however another port can be used.

### 3.4.7.2.3 Issue #2: Primary and Secondary license servers configured

In the Service Tools, in **Initial Configuration > Licensing > Floating License**, no licenses are displayed even though the Primary and the Secondary Floating License Server have been configured.



### 3.4.7.2.4 Solution issue #2

The Primary License server may have been shutdown or may have become defective.

In **Initial Configuration > Licensing > CoLA Server**, check the following:

- Click on the Target Server link on top of the Floating License Manager screen.



- Check that the Floating License Manager screen displays the licenses available on the Secondary license server.



- Warn the IT Admin that the Primary license server is down and must be restarted and/or fixed.

### 3.4.7.3 CardIQ Xpress Process does not generate series

After installing CardIQ Xpress Process, the CXP application might not work (i.e. no series are generated by CXP). it might be necessary to restart Preprocessing service to correct this issue.

Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#) to restart all services.

#### NOTE

Warn the users then put the server in maintenance mode before performing the restart of services, as AW Server will be unavailable during restart.

### 3.4.7.4 2D Viewer does not launch

#### 3.4.7.4.1 Issue

On AW Server 3.0 Ext.2.0 and prior versions, when the ViewerManager exits, some libraries are deleted causing the 2D Viewer to be unable to restart.

#### 3.4.7.4.2 Workaround

In this case, it is necessary to reinstall the missing libraries from the RPM package, from the platform media that was used for the installation, as follow:

- Put the AW Server in maintenance mode to avoid conflicts on files being used.
- For each RPM package and the corresponding name and location in AWS:

RPM Package	File/Directory Path in RPM	File/Directory Location in AWS
aia-OVNILibraries	./export/home/sdc/AIA/OVNI/CommonLib_x86_64	/export/home/sdc/AIA/OVNI
aia-CommonLibrary *	./export/home/sdc/AIA/CommonLib_x86_64	/export/home/sdc/AIA
aia-awViewer **	./export/home/sdc/AIA/OVNI/awViewer/bin_x86_64	/export/home/sdc/AIA/OVNI

\*Perform below step for aia-CommonLibrary package and not for other package containing this name.

\*\*Perform below step for aia-awViewer package and not for other package containing this name.

Use **rpm2cpio** command to extract the file/directory from the RPM package mentioned previously and copy them at the right location.

See [A.23 RPM2CPIO on page 528](#) for the full procedure.

#### **NOTE**

The package name (first column) is truncated. The full name of the package contains the version.

3. Restart all services.

Follow instructions in [3.4.1.8 Software Subsystem Restart on page 164](#).

### **3.4.7.5 System could not supply enough resources for Volume Viewer**

**Problem:** On AW Server 3.2 Ext. 3.2 the message `System could not supply enough resources` is displayed when starting Volume Viewer application in the following configuration:

- **SdC\_High\_Tier\_Premium** license used
- **Volume Viewer** installed (all versions)

**Solution:** To avoid this issue update the `/usr/share/jumai-bin/start.sliceCountUtils` file:

1. Put the AW Server in maintenance mode, to guarantee there is no user connected to server, as restart will be necessary.
2. Open the AW Server Console/terminal, login as `root`.
3. Update the `start.sliceCountUtils` file with the following commands:

```
cd /usr/share/jumai-bin <Enter>
cp start.sliceCountUtils start.sliceCountUtils.orig <Enter>
sed -i 's/SdC_Nano_|SdC_Nano_|SdC_High_Tier_Premium/' \
start.sliceCountUtils <Enter>
```

4. Check that `SdC_High_Tier_Premium` was added to the end of the line that displays with the following command:

```
diff start.sliceCountUtils start.sliceCountUtils.orig | head -2 <Enter>
```

5. Reboot the AW Server:

```
reboot <Enter>
```

6. When reboot is complete, exit the maintenance mode.

### **3.4.7.6 Graphic performance degraded when paging in Volume Viewer**

**Problem:** On AW Server 3.2, when paging on reformatted view in Volume Viewer with a big number of volumes (greater than 20), after a while the paging performance is degraded and user experiences images lagging.

**Limitation:** This configuration change cannot be applied with AW Server configured in a **Seamless integration mode**.

**Solution:** To avoid this issue, change Volume Viewer configuration by modifying volume viewer launch script file, as follow:

1. Open the AW Server Console/terminal, login as **sdc / adw2.0**.
2. Update Volume Viewer configuration file, by removing the `setenv VXTL_SYNC_MULTIVOLUME` line, as follow:

```
cd /export/home/sdc/vxtl/bin <Enter>
cp start_volan start_volan.orig <Enter>
sed -i '/setenv VXTL_SYNC_MULTIVOLUME/d' start_volan <Enter>
```

3. Verify that only this line has been modified:

```
diff start_volan start_volan.orig <Enter>
```

The following line should be displayed:

```
> setenv VXTL_SYNC_MULTIVOLUME
```

### 3.4.7.7 Applications interactive performance degradation

**Problem:** On AW Server 3.2 Ext. 3.4 and previous releases, switching the PNF off and on duplicates the firewall rules and leads to network performance degradation. And as a consequence, the interactive performance of the applications are degraded (i.e.: paging becomes slow in Volume Viewer or Reformat...).

To confirm such performance degradation of the applications, type the following command:

```
conf | grep SYN-FLOOD <Enter>
```

The result should be as:

```
SYN-FLOOD tcp -- 0.0.0.0/0 0.0.0.0/0 tcp
flags:0x17/0x02
Chain SYN-FLOOD (4 references)
```

With more than one reference for the `Chain SYN-FLOOD` (here four references).

**Solution:** To fix the issue and prevent it from reoccurring:

1. Open the AW Server Console/terminal, login as **root**.
2. Stop the firewall:

```
service pnf off <Enter>
```

3. Type the following commands:

```
cd /usr/share/gehc_security/pnf/scripts <Enter>
echo "#Remove rules added by SYN FLOOD protection" >> flush.sh <Enter>
echo "iptables -F SYN-FLOOD" >> flush.sh <Enter>
echo "ip6tables -F SYN-FLOOD" >> flush.sh <Enter>
echo "iptables -D INPUT -p tcp --syn -j SYN-FLOOD" >> flush.sh <Enter>
echo "ip6tables -D INPUT -p tcp --syn -j SYN-FLOOD" >> flush.sh <Enter>
echo "iptables -X SYN-FLOOD" >> flush.sh <Enter>
```

- ```
echo "ip6tables -X SYN-FLOOD" >> flush.sh <Enter>
```
4. Clear the firewall rules:

```
iptables -F <Enter>
```

 5. Restart the firewall:

```
service pnf on <Enter>
```

3.4.7.8 Dotmed communication causes AW Server performance degradation when loading many volumes in Volume Viewer

Problem: On AW Server 3.2, when many volumes (exams & series) are loaded in Volume Viewer, the Dotmed communication information are increasing, which causes performances degradation when scrolling/paging in Volume Viewer and, more generally, causes AW Server performances issues.

NOTE

This issue is fixed in Volume Viewer Applications 17.0 Ext. 2 (vxtl_17.0-2.65).

For the moment, this workaround is not applicable for the environments that still require dotmed: Interventional, Inline MR, and UV seamless.

Solution: To eliminate this issue, change following Volume Viewer configuration files:

1. Open the AW Server Console/terminal, login as **sdc**.
2. Backup the original file:

```
cd /export/home/sdc/vxtl/bin <Enter>
cp start_appli.awe start_appli.awe.orig <Enter>
```

3. Update the `start_appli.awe` file by disabling the `VXTL_SYNC_MULTIVOLUME` environment variable:

```
sed -i 's/^\(.*setenv VXTL_SYNC_MULTIVOLUME\)/#\1/' start_appli.awe
<Enter>
```

4. Verify that the `start_appli.awe` file is updated correctly:

```
diff start_appli.awe start_appli.awe.orig <Enter>
```

The following lines appear:

```
<# setenv VXTL_SYNC_MULTIVOLUME
---
```

```
> setenv VXTL_SYNC_MULTIVOLUME
```

5. Create the `.vxtl_custom_config.csh` file and add the `VXTL_SPATIAL_POSITION_SYNC_OFF` environment variable:

```
cd <Enter>
```

```
echo "setenv VXTL_SPATIAL_POSITION_SYNC_OFF" > .vxtl_custom_config.csh
<Enter>
```

6. Verify that the `.vxtl_custom_config.csh` file is created correctly:

```
cat .vxtl_custom_config.csh <Enter>
```

The following line appears:

```
setenv VXTL_SPATIAL_POSITION_SYNC_OFF
```

3.4.7.9 Cannot launch applications in Hybrid integration mode with the PACS 3rd party integrated AW Server Client

Problem: In Hybrid integration mode (3rd party integration mode), the SmartScore, Advantage4D and GSI Viewer applications cannot be started. The series selection panel is, at first, empty. Then after some period of time (several minutes – May be longer if there are more exams in the AW Server database), every series from all patients appears in the series selection panel.

The problem only happens in Hybrid integration mode (3rd party integration mode). It does **not** happen when 3rd party front-end integration is used together with DICOM Direct Connect (AW Enterprise).

Solution 1: To eliminate this issue, instead of using the PACS 3rd party integrated AW Server Client, use the AW Server Client from the PC:

1. Install the AW Server Client on the PC.
2. Start the AW Server Client.
3. Select appropriate Patient/Exam/Series in AW Server Patient List.
4. Start the application (SmartScore, Advantage4D and GSI Viewer).

NOTE

This workflow provides similar result compared to PACS 3rd party integrated AW Server Client. The additional step is to launch AW Server Client separately and select again data to review from AW Server Patient List.

Solution 2: To eliminate this issue, use the PACS 3rd party integrated AW Server Client with selection at series level:

NOTE

Solution 2 is not applicable to GSI Viewer application.

1. Configure the PACS frontend so that the PACS 3rd party integrated AW Server Client starts on a specified series.

Refer to the *AWS3.2 PACS Integration Guide 5535310-1EN* for a detailed explanation on the PACS frontend configuration.

NOTE

For RA1000, it is possible to use several selection levels by selecting either a study or selecting specific series on RA1000 graphical user interface. However, in this workaround study selection should **never** be used.

Use series selection level for Advantage4D and SmartScore. Use any selection level for other applications.

2. Starts the PACS 3rd party integrated AW Server Client on a specified series.
3. For troubleshooting purpose, the integration command parameters can be checked on the client side logfiles at %appdata%\Solo\[clientinstallUUID]\integration_logs\integration.log and/or at %appdata%\Solo\[clientinstallUUID]\logs*_global.log.

integration.log shows the received parameters with the integration.exe call, and also shows result codes of the execution.

The path to any AW Server Client log file contains the client instance id (earlier referred as clientinstallUUID) for the client installation, which is a unique identifier. This is used to separate the contents of different AW Server Client installations. This ID can be found in the AW Server Client install directory in file solo\client_instance_id.txt.

The integration command launched will look like the below command using the series selection level (using the `-selectedSeries` parameter):

```
integration.exe -apiVersion=2.0 -loginLaunch
-awServerIP=10.0.0.1 -user=johndoe -secure=yes
-selectedStudy=2.25.90736046944774348264090248490730691254
-selectedSeries=2.25.71672780338002721509762338971556836384 -uniqueID=1
```

For any help on integration command troubleshooting contact the OLC.

On certain PACS it is not possible to use series selection level. If the particular PACS does not support series level selection, please use Workaround **Solution 1**.

3.4.7.10 Logging-out from AW Server Client causes AW Server performance degradation

Problem: On AW Server 3.2, when logging-out from AW Server Client, the MiniViewer session may continue to run and becomes a Zombie process in the system. When too many MiniViewer Zombie processes are running, they can take 100% of a CPU and cause the AW Server performance degradation.

Detection: To check that the issue faced is the one described above, identify if MiniViewer Zombie processes are running:

1. Open the AW Server Console/terminal, login as **sdc**.
2. Display the MiniViewer Zombie processes:

```
pgrep -u sdc -P 1 -f previewPane <Enter>
```

If several lines containing number (they are the MiniViewer Zombie processes numbers) display, then the issue occurred.

Solution: To eliminate this issue, kill the MiniViewer Zombie processes:

1. Using the AW Server Console/terminal, kill the MiniViewer Zombie processes:

```
kill -9 `pgrep -u sdc -P 1 -f previewPane` <Enter>
```

2. Verify that no more MiniViewer Zombie process are running:

```
pgrep -u sdc -P 1 -f previewPane <Enter>
```

No result should display.

3. To avoid reoccurrence of the issue and to prevent reexecuting the above steps:

- a. Open the cron table file:

```
crontab -e <Enter>
```

- b. The cron table file opens using "**vi**" editor. Go to the end of the file using the **<Down arrow>** key then press the **<o>** key to insert a line in the file.

- c. Copy/paste the below line to the end of the cron table file:

```
40 1 * * * kill -9 `pgrep -u sdc -P 1 -f previewPane`
```

- d. Press **<Esc>** then **:wq** to save the file and exit.

- e. Verify the content is as intended in crontab configuration by typing:

```
crontab -l <Enter>
```

The line added above should be present in the output of the command.

3.4.7.11 Some Volume Viewer shortcuts are executed twice when Volume Viewer is started with Web Access

Problem: Volume Viewer does not manage properly the shortcuts actions when they are sent from Web Access mode. For instance, when sending an image to the Filmer (using F1 shortcut), the image is sent twice.

Solution: To eliminate this issue, the `shortcutsPreferenceAW.xml` and `shortcutsPreference_phx.xml` files must be updated:

1. Open the AW Server Console/terminal, login as `sdc`.
2. Navigate to the `/export/home/sdc/vxtl/protocols` directory:

```
cd /export/home/sdc/vxtl/protocols <Enter>
```

3. Backup the original files:

```
cp shortcutsPreferenceAW.xml shortcutsPreferenceAW.xml.orig <Enter>
```

```
cp shortcutsPreference_phx.xml shortcutsPreference_phx.xml.orig <Enter>
```

4. In `shortcutsPreferenceAW.xml` file, using "`vi`" editor, add "autoRepeat="false"" at the end of the following lines:

NOTE

To navigate in the file use the `<arrow>` keys. To enter the editor mode (to insert text) use the `<i>` key. To exit the editor mode use `<Esc>` key.

```
vi shortcutsPreferenceAW.xml <Enter>
```

```
<shortcut key="FilmFromKey" keyboardAction="KeyRelease+F1"
action="FilmFromKey()" autoRepeat="false"/>
```

```
<shortcut key="FilmPageFromKey" keyboardAction="KeyRelease+F2"
action="FilmPageFromKey()" autoRepeat="false"/>
```

```
<shortcut key="FilmMidFromKey" keyboardAction="KeyRelease+F3"
action="FilmMidFromKey()" autoRepeat="false"/>
```

```
<shortcut key="SwitchMouseModeFromKey" keyboardAction="KeyRelease+Tab"
action="SwitchMouseModeFromKey()" autoRepeat="false"/>
```

5. To save the file and exit type `:wq` then press `<Enter>`.

6. In `shortcutsPreference_phx.xml` file, using "`vi`" editor, add "autoRepeat="false"" at the end of the following lines:

```
vi shortcutsPreference_phx.xml <Enter>
```

```
<shortcut key="DeleteTraceFromKey" keyboardAction="Ctrl+KeyRelease+u"
action="DeleteWfFromKey()" autoRepeat="false"/>
```

```
<shortcut key="LocalRegistrationFromKey" keyboardAction="KeyRelease+X"
action="LocalRegistrationFromKey()" autoRepeat="false"/>
```

```
<shortcut key="ExportSequenceFromKey" keyboardAction="KeyRelease+F4"
action="ExportSequenceFromKey()" autoRepeat="false"/>
```

```
<shortcut key="ShowHideCursorFromKey" keyboardAction="KeyRelease+C"
action="ShowHideCursorFromKey(toggle)" autoRepeat="false"/>
```

```
<shortcut key="QuickAVAFromKey" keyboardAction="KeyRelease+Q"
action="QuickAVAFromKey()" autoRepeat="false"/>
```

```

<shortcut key="AutofitVRFromKey" keyboardAction="KeyRelease+A"
action="AutofitVRFromKey()" autoRepeat="false"/>

<shortcut key="AutoScaleFromKey" keyboardAction="Alt_L+KeyRelease+G"
action="AutoScaleFromKey()" autoRepeat="false"/>

<shortcut key="ManualRegistrationFromKey" keyboardAction="KeyRelease+M"
action="ManualRegistrationFromKey()" autoRepeat="false"/>

<shortcut key="ShowMidSegmentPointFromKey" keyboardAction="KeyRelease+G"
action="ShowMidSegmentPointFromKey()" autoRepeat="false"/>

<shortcut key="ToggleLabelX" keyboardAction="KeyRelease+E"
action="ToggleLabelX()" autoRepeat="false"/>

<shortcut key="StopCTCJoystickFromKey" keyboardAction="KeyRelease+space"
action="StopCTCJoystickFromKey()" autoRepeat="false"/>

<shortcut key="CollapsePanelFromKey" keyboardAction="KeyRelease+space"
action="" autoRepeat="false"/>

<shortcut key="DeleteTraceFromKey" keyboardAction="Ctrl+KeyRelease+u"
action="DeleteWfFromKey()" autoRepeat="false"/>

```

- To save the file and exit type :wq then press <Enter>.

3.4.7.12 SmartScore custom templates are not saved correctly

Problem: SmartScore does not store the custom templates when it closes. SmartScore stores custom templates in a temporary folder. When it closes, SmartScore uses the Linux command “rsync” to synchronize this temporary folder and store the templates permanently. The “rsync” command is missing on the system, therefore the synchronization fails and the templates are not stored permanently.

Solution: To eliminate this issue, extract the “rsync” package from the OS iso and install it:

- Insert the OS media into the client PC or the FE laptop.
- Map the OS iso file to the virtual CD/DVD drive, through the iLO for a Physical AW Server or the hypervisor for a Virtual AW Server.
- Open the AW Server Console/terminal, login as **root**.
- Mount the OS iso file using the following commands:

```
mkdir -p /mnt/media <Enter>
```

Virtual AW Server:

```
mount /dev/cdrom /mnt/media <Enter>
```

Physical AW Server:

```
mount /dev/sr1 /mnt/media <Enter>
```

- Navigate to the /mnt/media/Packages directory:

```
cd /mnt/media/Packages <Enter>
```

- Install the “rsync” package:

```
rpm -i rsync-3.1.2-6.el7_6.1.x86_64.rpm <Enter>
```

- Verify that the “rsync” package is installed:

```
rpm -qa | grep rsync <Enter>
```

The following line appear:

```
rsync-3.1.2-6.el7_6.1.x86_64
```

8. Unmount the OS iso file:

```
cd <Enter>
```

```
umount /mnt/media <Enter>
```

9. Disconnect the OS iso file:

Virtual AW Server:

```
eject cdrom <Enter>
```

Physical AW Server:

```
eject sr1 <Enter>
```

3.4.7.13 Scrolling is slow and choppy in Volume Viewer viewport within Universal Viewer

Problem: In Universal Viewer (UV) environment, the scrolling behavior in Volume Viewer viewport is slow and choppy. This significant lag, while scrolling in viewports, is due to the cursor synchronization between the Universal Viewer and the AW Server.

Solution: To eliminate this issue, disable the cursor synchronization between the Universal Viewer and the AW Server:

1. In the Universal Viewer, navigate to the C:\Program Files (x86)\Integrad.3\MIV folder.
2. Edit the `integrations.ini` file.
3. Locate the section of the file labeled [HAWAII].
4. At the end of the section, add the line:

```
SCROLL_SYNC=<value>
```

Replacing `<value>` with one of the following:

- 0
- n
- no
- -
- false

NOTE

If the value of `SCROLL_SYNC` is anything other than the values listed above, or if the `integrations.ini` file does not contain a `SCROLL_SYNC` line, the cursor synchronization will be enabled.

5. The section labeled [HAWAII] in the integrations.ini file, should look like:

```
[HAWAII]
ISENABLED=1
IWSERVERURL=http://3.28.245.207/services/PacsWebService
AWSERVERURL=http://3.28.245.4
TOKEN=STUB_TOKEN_0
WINDOWWIDTH=850
WINDOWHEIGHT=670
REARENTPLUGIN=1
SOLOMINIDEBUG=0
HEIGHTTOWIDTHRATIO=0.8
WINDOWWIDTHPERCENT=60
MAXHORZRESOLUTION=1600
MAXVERTRESOLUTION=1200
SOLO_CLIENT_PATH=C:\Program Files\GE\AWS_2.0\solo
SCROLL_SYNC=0
```

NOTE

In this example, the SCROLL_SYNC value has been set to “0” (zero).

3.4.8 Cybersecurity support

| Applicability* | AW Server 3.2 Extension | | | | | | | | | | | |
|---|-------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | 1.0 | 1.2 | 2.0 | 3.0 | 3.2 | 3.4 | 4.0 | 4.2 | 4.4 | 4.6 | 4.8 | 4.9 |
| 3.4.8.1 Cyber-attack on the AW Server system on page 270 | X | X | X | X | X | X | X | X | X | X | X | X |
| 3.4.8.2 CoLA license server cybersecurity support on page 271 | X | X | X | X | X | X | X | X | X | X | X | X |
| 3.4.8.3 Security vulnerability in Apache's Log4J2 component on page 289 | | | | | | | | X | | | | |
| 3.4.8.4 SSL cypher security level too low on page 290 | | | | | | | X | | | | | |

*An empty cell means the problem is not present or has been fixed in the corresponding extension.

NOTE

In the below workarounds when a file is updated, it is requested to backup it (copy the file into <filename>.orig – the extension may differ). So, if some mistakes occur while executing the workarounds, it is recommended to recover the backup file (copy the backup file into the original file) and to re-execute the workaround.

3.4.8.1 Cyber-attack on the AW Server system

Problem: The hospital encountered a cyber-attack on his network. Such attack can affect the Apache Web servers, which lead to potential intrusions on the AW Server system.

Solution: To prevent any intrusion on the AW Server system, disconnect the users using the AW Server with the following instructions:

1. Open the AW Server Console/terminal, login as **root**.
2. Execute the following command:
Systemctl stop httpd service <Enter>
3. Immediately inform the users/customer about the system's unavailability.
4. The AW Server should be disconnected from the network and/or powered off to prevent any further malicious activity.

3.4.8.2 CoLA license server cybersecurity support

Problem: The CoLA license server encounters some vulnerabilities due to:

- Exposure of CoLA license server port in case of standalone licensing mode (i.e. when the CoLA server runs on an AW Server and only provides licenses to this local AW Server).
- Lack of encrypted communication between the server and the client side in case of centralized licensing mode (i.e. when the CoLA server provides licenses to several AW Servers).
- Weakness of the Apache UI component in case of centralized licensing mode with the CoLA 3.3.1 License Server installed on Windows. This UI component allows the user to manage licenses, check the connected clients and check the log files.

Solution: To prevent potential cybersecurity issues:

- In case of standalone licensing mode, the script that opens the CoLA server port in the firewall at each reboot must be modified to stop doing it. Refer to [3.4.8.2.1 Standalone licensing mode for AW Server 3.2 Ext. 4.0 \(and higher releases\) on page 271](#) or [3.4.8.2.3 Standalone licensing mode for AW Server 3.2 Ext. 3.4 \(and prior releases\) on page 279](#).
- In case of centralized licensing mode, the AW Server and CoLA server must be configured to communicate between themselves using a TLS tunneling service (e.g.: a stunnel). To restrict the unauthorized access of the Windows based CoLA license server, remote access with internet browser must be disabled. Refer to [3.4.8.2.2 Centralized licensing mode for AW Server 3.2 Ext. 4.0 \(and higher releases\) on page 271](#) or [3.4.8.2.4 Centralized licensing mode for AW Server 3.2 Ext. 3.4 \(and prior releases\) on page 280](#).
- In case of security vulnerability with the Apache UI component on the CoLA 3.3.1 License Server installed on Windows, either ask the Customer IT admin to block the port 80 on the firewall or stop and uninstall the Apache server then remove the Apache component. Refer to [3.4.8.2.5 Fixing the CoLA License Server security vulnerability with the Apache UI on Windows on page 288](#).

3.4.8.2.1 Standalone licensing mode for AW Server 3.2 Ext. 4.0 (and higher releases)

1. Open the AW Server Console/terminal and login as **root**.
2. Navigate to the `/usr/share/gehc_security/pnf/pnfcustomscripts` directory:
`cd /usr/share/gehc_security/pnf/pnfcustomscripts <Enter>`
3. Modify the script to prevent the opening of CoLA server port (17767) in the firewall:
`cp modality.sh modality.sh.orig <Enter>`
`sed -e '/[|]cola/ s/^#*/#/g' -i modality.sh <Enter>`
4. Restart the firewall:
`systemctl restart pnf <Enter>`
5. Verify that the port 17767 is closed by typing the following command and checking the port 17767 is in the output:
`iptables -L <Enter>`

3.4.8.2.2 Centralized licensing mode for AW Server 3.2 Ext. 4.0 (and higher releases)

The following subsections describe the configuration of the communication between the AW Server and the CoLA server using a TLS tunneling service (e.g.: a stunnel).

3.4.8.2.2.1 Configuring the AW Server 3.2 Ext. 4.0 (or higher releases) used as a CoLA server

1. Open the AW Server Console/terminal and login as **root**.

2. Stop the CoLA service:

```
systemctl stop cola-server.service <Enter>
```

3. Generate a new common pem file **cola.pem**, which will be used for stunnel communication:

- a. Type the following command to package the **cola.pem** file:

```
/usr/sbin/certgen.sh -z <Enter>
```

- b. Enter a password and note it.

The **cola.pem** file is zipped and moved to **/var/lib/tomcat/webapps/awe/client/cola.pem.zip**.

4. Configure the CoLA server using a stunnel communication:

```
/usr/sbin/stunnelsetup.sh -s --cola-reconfig -f on <Enter>
```

5. Restart the CoLA service:

```
systemctl restart cola-server.service <Enter>
```

6. From the Service Tools, select **Initial configuration > Licensing > CoLA Server**.

7. Check that the AW Server is configured as a CoLA server with **Server Port** set to 17768.



8. From the Service Tools, select **Initial configuration > Licensing > Floating License**.

9. Check that the applications licenses are available.

| Licenses On Media: | | | Licenses On Server: | | | |
|-------------------------|-------------|-------|--------------------------|-------------------------|------------------|-------|
| License Key String | License Key | Users | Del | License Key String | License Key | Users |
| AutoBone_Xpress | | | <input type="checkbox"/> | AutoBone_Xpress | 99CD2UMOAFL3MREH | 5 |
| Integrated_Registration | | | <input type="checkbox"/> | Integrated_Registration | OTPF2KRXBLODYKGM | 5 |
| OncoQuant | | | <input type="checkbox"/> | OncoQuant | 7YH2W3WLSB628PAC | 5 |
| PET_VCAR | | | <input type="checkbox"/> | PET_VCAR | AQGBY8RS968KKDFY | 5 |
| Volume_Viewer | | | <input type="checkbox"/> | Volume_Viewer | 94ZT8MG94JRXJF3Z | 5 |

<- -> Update Server Check All Clear All Delete
 File: Choose File No file chosen Read Media
 Copyright ©2005-2014 GE Healthcare

After each AW Server used as CoLA client is configured (see [3.4.8.2.2 Configuring the AW Server Ext. 4.0 \(or higher releases\) used as a CoLA client on page 273](#)), the `cola.pem.zip` file doesn't need to be distributed to other systems. To delete it, type:

```
rm /var/lib/tomcat/webapps/awe/client/cola.pem.zip <Enter>
```

3.4.8.2.2 Configuring the AW Server Ext. 4.0 (or higher releases) used as a CoLA client

1. Open the AW Server Console/terminal and login as **root**.
2. Stop the CoLA service:

```
systemctl stop cola-server.service <Enter>
```

3. Navigate to the `/etc/stunnel` directory:

```
cd /etc/stunnel <Enter>
```

4. Copy the common `cola.pem.zip` file from the AW Server configured as a CoLA Server (see [3.4.8.2.1 Configuring the AW Server 3.2 Ext. 4.0 \(or higher releases\) used as a CoLA server on page 272](#)) and extract it to the `/etc/stunnel` directory:

- a. Type the command:

```
/usr/sbin/certgen.sh --dzip <AWS1_IP> <Enter>
```

Where `<AWS1_IP>` is the IP address of the AW Server configured as a CoLA Server.

- b. Use the password noted in [3.4.8.2.1 Configuring the AW Server 3.2 Ext. 4.0 \(or higher releases\) used as a CoLA server on page 272](#).
- c. If requested, replace the `cola.pem` file.

NOTE

If the common `cola.pem` file is located on a Windows CoLA Server, use the `scp` or `winscp` command to copy the file to the `/etc/stunnel` directory.

- Configure the AW Server as a CoLA client:

```
/usr/sbin/stunnelsetup.sh -c --host1 <AWS1_IP> <Enter>
```

NOTE

Configure the second CoLA Server by appending the **--host2 <AWS2_IP>** option to the above command, where **<AWS2_IP>** is the IP address of the second CoLA Server.

Download the **cola.pem.zip** file on the AW Server by appending the **--dzip <AWS1_IP>** option to the above command.

- Restart the CoLA service:

```
systemctl restart cola-server.service <Enter>
```

- From the Service Tools, select **Initial configuration > Licensing > CoLA Server**.

- Check that the AW Server is configured as a CoLA server with **Server Port** set to 7777.



- From the Service Tools, select **Initial configuration > Licensing > Floating License**.

- Check that the applications licenses are available.

| Licenses On Media: | | | Licenses On Server: | | | |
|-------------------------|-------------|-------|--------------------------|-------------------------|------------------|-------|
| License Key String | License Key | Users | Del | License Key String | License Key | Users |
| AutoBone_Xpress | | | <input type="checkbox"/> | AutoBone_Xpress | 99CD2UMOAFL3MREH | 5 |
| Integrated_Registration | | | <input type="checkbox"/> | Integrated_Registration | OTPF2KRXBLODYKGM | 5 |
| OncoQuant | | | <input type="checkbox"/> | OncoQuant | 7YH2W3WLSB628PAC | 5 |
| PET_VCAR | | | <input type="checkbox"/> | PET_VCAR | AQGBY8RS968KKDFY | 5 |
| Volume_Viewer | | | <input type="checkbox"/> | Volume_Viewer | 94ZT8MG94JRXJF3Z | 5 |

<- > Update Server Check All Clear All Delete
 File: Choose File No file chosen Read Media

New License Installation:

License Key String: License Key:

Copyright ©2005-2014 GE Healthcare

When each AW Server is configured as a CoLA client, make sure that the original source file **cola.pem.zip** is removed from the CoLA Server (see [3.4.8.2.2.1 Configuring the AW Server 3.2 Ext. 4.0 \(or higher releases\) used as a CoLA server on page 272](#)).

3.4.8.2.2.3 Configuring the CoLA server on Windows

The CoLA server must be already installed. If not, refer to the Floating License 3.3.x Installation Manual 5537368-1EN.

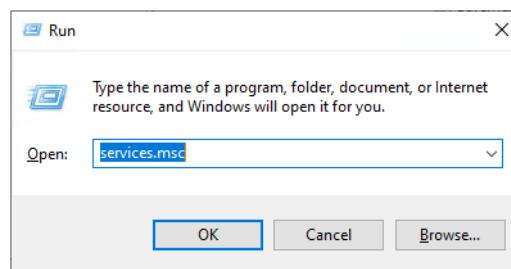
1. Follow [Step 2 to Step 12](#) to configure CoLA and the tunneling service.
2. Open a Command Prompt.
3. Update the CoLA server license port in the file `c:\Program Files\gemsLicenseServer\config\Cola_Config.txt`:
 - a. Edit the file using the Notepad editor.
 - b. Replace

LICENSE_PORT=17767

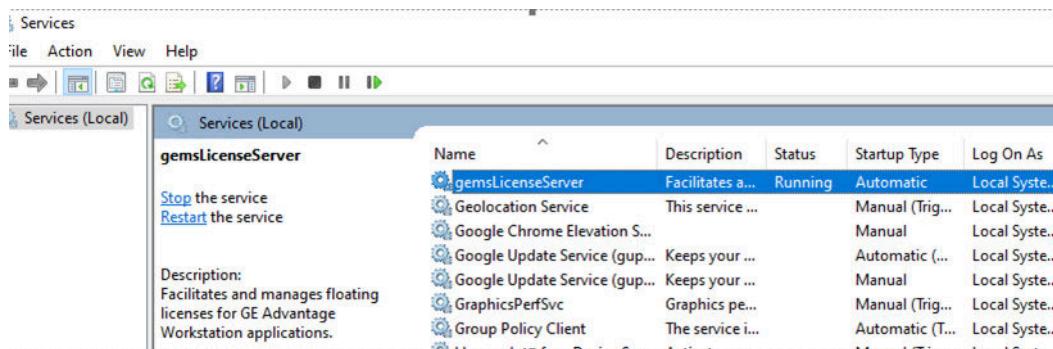
by

LICENSE_PORT=17768

4. Restart gemsLicenseServer Windows service or restart the system to apply port allocation:
 - a. Press `<Win> + <R>` to open the Run dialog.
 - b. Execute `services.msc` to open the Services window.



- c. Right-click on **gemsLicenseServer** and select **Restart**.



5. Download the tunneling service package for Windows from <https://www.stunnel.org/downloads.html>.

The screenshot shows the official stunnel project website. At the top, there is a navigation bar with links for About, Documentation, Examples, Vulnerabilities, Downloads, and COPY. Below the navigation bar is a decorative banner featuring binary code. A table titled "Latest Version" lists six files for download:

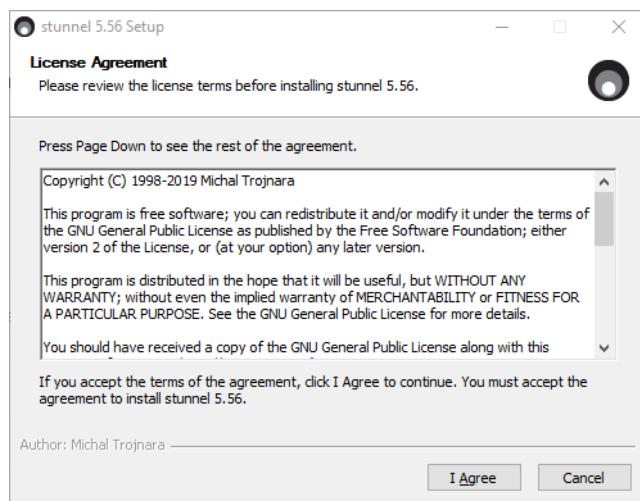
| File Name | Size | Date |
|---|---------|--------------------|
| stunnel-5.56-android.zip | 1414761 | 22nd November 2019 |
| stunnel-5.56-android.zip.asc | 963 | 22nd November 2019 |
| stunnel-5.56-android.zip.sha256 | 91 | 22nd November 2019 |
| stunnel-5.56-win64-installer.exe | 2870104 | 22nd November 2019 |
| stunnel-5.56-win64-installer.exe.asc | 963 | 22nd November 2019 |
| stunnel-5.56-win64-installer.exe.sha256 | 99 | 22nd November 2019 |

6. Install the `stunnel-5.56-win64-installer.exe` package:

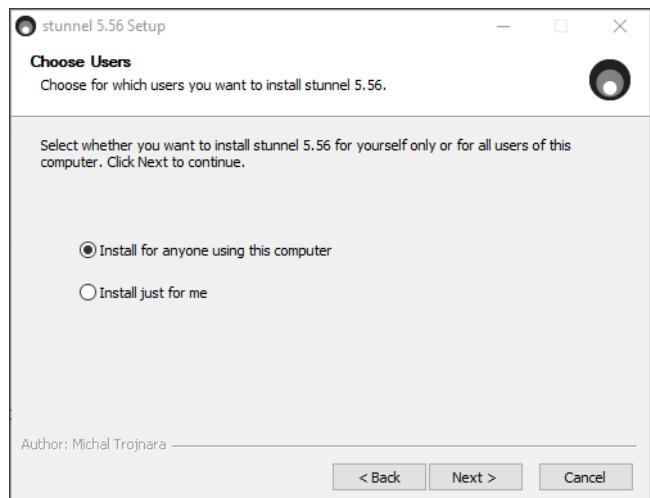
NOTE

If Openssl asks certificate relevant questions, add a dummy values as certificate is managed from the AW Server side.

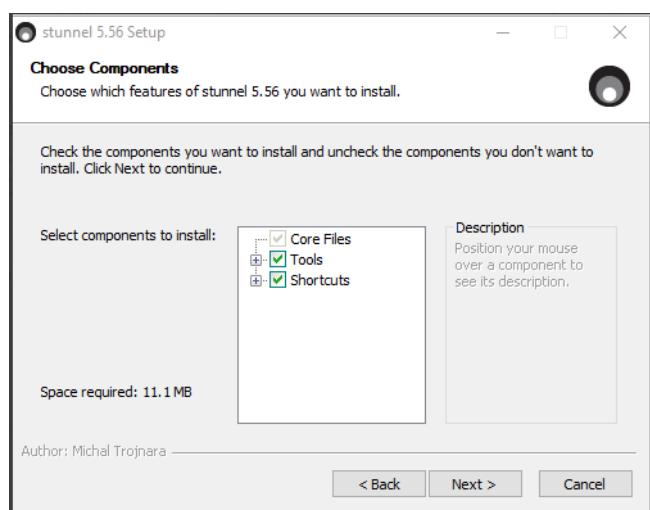
- When the License Agreement appears, click on **I Agree**.



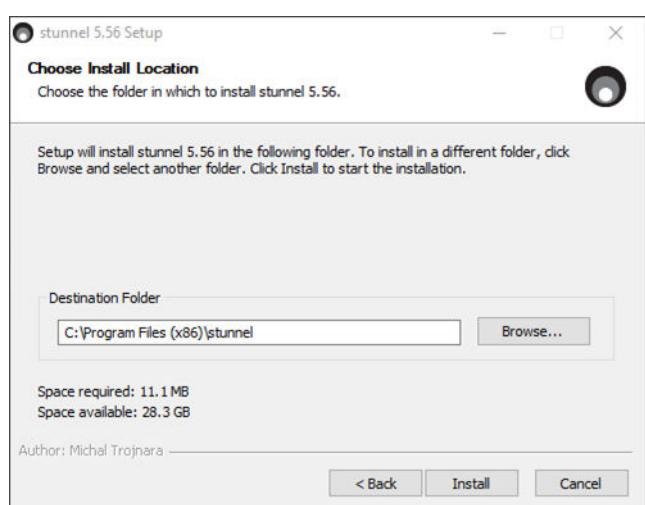
- On the Choose Users panel, keep selection and click on **Next**.



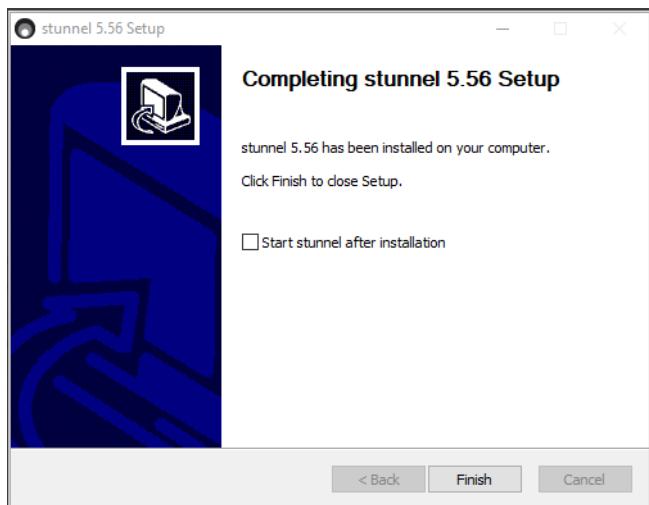
- c. On the *Choose Components* panel, keep selection and click on **Next**.



- d. On the *Choose Install Location* panel, keep destination folder and click on **Install**.



- e. When the installation is completed check **Start stunnel after installation** and click on **Finish**.

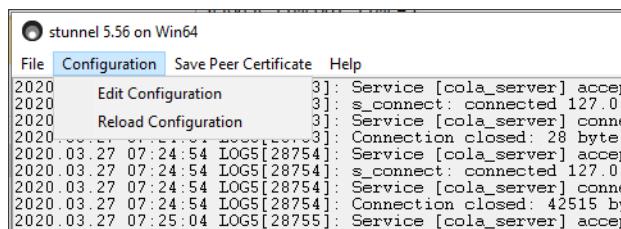


7. NOTE

This is an optional step - in case it is not done previously.

From the AW Server used as licensing client, where the certificate is generated, copy the file /etc/stunnel/cola.pem to C:\Program Files (x86)\stunnel\config using SCP or WinSCP.

8. From the stunnel user interface, edit the configuration file by selecting **Configuration > Edit Configuration:**



9. Update the SSL version in the configuration file:

Replace

```
sslVersion = ...
sslVersionMax = ...
```

by

```
sslVersionMax = TLSv1.2
sslVersion = TLSv1.2
```

10. Delete all lines related to client and server mode services:

```
***** Example TLS client mode services
```

and

```
***** Example TLS server mode services
```

11. Copy the following text and paste it at the end of the file:

```
[cola_server]
accept=17767
connect = 17768
cert = cola.pem
CAfile=cola.pem
verify=3
```

12. From the stunnel user interface, select **Configuration > Reload Configuration**.

In the stunnel user interface, at the bottom of the log, Configuration successful appears.

13. Follow [Step 14](#) to [Step 16](#) to configure the Apache server and revoke remote access.

It will restrict the local access in order to make the configuration of the licenses more secure.

14. Update the file C:\Program Files\gemsLicenseServer\Apache2\conf\httpd.conf:

- a. Edit the file using the Notepad editor as Administrator.
- b. Search for the following section:

```
<Directory "C:/PROGRA~1/gemsLicenseServer/Apache2/cgi-bin">
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>
```

- c. Replace

```
Allow from all
```

by

```
Allow from 127.0.0.1
```

15. Update the shortcut **FL Service Menu** on the Desktop of the user by replacing the URL

<http://<IP>:80/cgi-bin/smain.cgi> by <http://localhost/cgi-bin/smain.cgi>.

16. Restart the Apache Windows service or restart the system to apply the changes.

Proceed as described in [Step 4](#) (replacing the gemsLicenseServer Windows service by the Apache Windows service).

3.4.8.2.3 Standalone licensing mode for AW Server 3.2 Ext. 3.4 (and prior releases)

Modify the firewall behaviour, so that the CoLA server port is not open at each reboot, as follow:

1. Open the AW Server Console/terminal, login as **root**.

2. Navigate to the /usr/share/gehc_security/pnf/pnfcustomscripts directory:

```
cd /usr/share/gehc_security/pnf/pnfcustomscripts <Enter>
```

3. Modify the script to prevent the opening of CoLA server port (17767) in the firewall:

```
cp modality.sh modality.sh.orig <Enter>
```

```
sed -e '/[|]cola/ s/^#*/#/g' -i modality.sh <Enter>
```

4. Reboot the AW Server:

```
reboot <Enter>
```

5. Open the AW Server Console/terminal, login as **root**.

6. Restart pnf:

```
/etc/init.d/pnf off <Enter>
```

```
iptables -F <Enter>
```

```
/etc/init.d/pnf on <Enter>
```

7. Verify the port 17767 is closed. Type the following command in the terminal and check whether port 17767 is existing in the output:

```
iptables -L<Enter>
```

3.4.8.2.4 Centralized licensing mode for AW Server 3.2 Ext. 3.4 (and prior releases)

The following subsections describe the configuration of the communication between the AW Server and the CoLA server using a TLS tunneling service (e.g.: a stunnel).

3.4.8.2.4.1 Creating a tunneling service common certificate for AW Server 3.2 Ext. 3.4 (and prior releases)

During the installation, the FE creates a new common pem file on the CoLA server. This file is used only for stunnel communication. The FE has to copy this pem file to the AW Server at a specific location, and configure the stunnel to use this certificate instead of the standard one.

A common certificate is used across the CoLA client-server topology.

1. Open a Terminal tool and login as **root**.
2. Navigate to the /etc/stunnel directory:

```
cd /etc/stunnel <Enter>
```

3. Create the self-signed certificate:

```
openssl req -x509 -new -nodes -newkey rsa:2048 -sha256 -days 730 \
-keyout cola.pem -out cola.pem <Enter>
```

Fill the proper Country Name, State, Locality Name, Organization name, Organization unit.

Common name and email address can remain blank.

NOTE

To print the pem file content type:

```
openssl x509 -in cola.pem -noout -text <Enter>
```

4. Make sure that the owner of the server.conf and cola.pem files is only **root**:

```
chmod 400 cola.pem <Enter>
```

5. Copy the pem file to all AW Server using scp or other solution:

- a. In Service Tools, open the ssh terminal.

- b. Enable the ssh in Service Tools.

- c. Copy the pem file to the other nodes (AW Server as floating CoLA client, AW Server as floating CoLA server, Windows CoLA server). To copy to Windows, use WinScp.

```
scp ./cola.pem root@<IP>:/etc/stunnel <Enter>
```

where <IP> is the IP address of the AW Server as floating CoLA client, AW Server as floating CoLA server, Windows CoLA server.

- d. Disable the ssh in Service Tools.

3.4.8.2.4.2 Configuring the AW Server 3.2 Ext. 3.4 (or prior releases) used as a CoLA server

1. Open the AW Server Console/terminal, login as **root**.
2. Update the CoLA server license port in the file /usr/share/FL_SERVER/Cola_config.txt:

```
cd /usr/share/FL_Server <Enter>
cp Cola_config.txt Cola_config.txt.orig <Enter>
sed -i 's/LICENSE_PORT = 17767/LICENSE_PORT = 17768/' Cola_config.txt <Enter>
```

3. Restart the CoLA server:

```
/etc/init.d/cola stop <Enter>
```

NOTE

In case the CoLA server has never been activated on the AW Server (after clean install), an error message appears, as the CoLA service is not running. Ignore the error message.

```
/etc/init.d/cola start <Enter>
```

4. Update the SSL version in the file /etc/stunnel/server.conf:

```
cd /etc/stunnel <Enter>
cp server.conf server.conf.orig <Enter>
sed -i 's/sslVersion =.*/sslVersion = TLSv1.2/' server.conf <Enter>
```

5. Edit the file /etc/stunnel/server.conf:

```
vi server.conf <Enter>
```

6. Go to the last line and press the <o> key to edit the file.

7. Copy the following text and paste it at the end of the file:

```
[cola-server]
accept = 17767
connect = 17768
verify=3
cert=/etc/stunnel/cola.pem
CAfile=/etc/stunnel/cola.pem
```

8. Press <Enter> to add an empty line at the end of the file.

9. Press <Esc> then type :wq to save the file and exit.

10. Restart the tunneling service:

```
killall -9 stunnel <Enter>
stunnel /etc/stunnel/server.conf <Enter>
```

11. Configure the CoLA server on Service Tools:

- a. From the Service Tools, select **Initial configuration > Licensing > CoLA Server**.

The *CoLA Server Configuration* appears.



- b. Check the **Built-in** checkbox.
 - c. Enter the **Server Enabler** license key.
 - d. Set the **Server Port** to **17768**.
 - e. Click on the **Apply** button.
12. Reboot the AW Server:

```
reboot <Enter>
```

3.4.8.2.4.3 Configuring the AW Server 3.2 Ext. 3.4 (or prior releases) used as a CoLA client

1. Open the AW Server Console/terminal and login as **root**.
2. From the AW Server where the certificate is generated, copy the file /etc/stunnel/cola.pem to /etc/stunnel.

NOTE

This is an optional step - in case it is not done previously.

3. Update the SSL version in the file /etc/stunnel/server.conf:

```
cd /etc/stunnel <Enter>
cp server.conf server.conf.orig <Enter>
sed -i 's/sslVersion =.*sslVersion = TLSv1.2/' server.conf <Enter>
```

4. Edit the file /etc/stunnel/server.conf:

```
vi server.conf <Enter>
```

5. Go to the last line and press the <o> key to edit the file.
6. Copy the following text, and paste it at the end of the file (replace <PrimaryServer_IP> and <SecondaryServer_IP> by the licensing servers):

```
[cola-client]
client=yes
accept=7777
verify=3
cert=/etc/stunnel/cola.pem
CAfile=/etc/stunnel/cola.pem
failover=prio
connect = <PrimaryServer_IP>:17767
connect = <SecondaryServer_IP>:17767
TIMEOUTconnect=1
```

7. Press **<Enter>** to add an empty line at the end of the file.
8. Press **<Esc>** and type **:wq** to save the file and exit.
9. Restart the tunneling service:

```
killall -9 stunnel <Enter>
stunnel /etc/stunnel/server.conf <Enter>
```

10. Configure the CoLA server in Service Tools:

- a. From the Service Tools, select **Initial configuration > Licensing > CoLA Server**.

The *CoLA Server Configuration* panel appears.



- b. Set the **Server Port** to **7777**.
- c. Click on the **Apply** button.

NOTE

Sometimes it is not possible to disable the built-in license server in case it was enabled. When you reload the page, it is still enabled, but seems to be configured in the CoLA. The workaround is to mistype the license key and click on **Apply**.

3.4.8.2.4 Configuring the CoLA server on Windows

The CoLA server must be already installed. If not, refer to the Floating License 3.3.x Installation Manual 5537368-1EN.

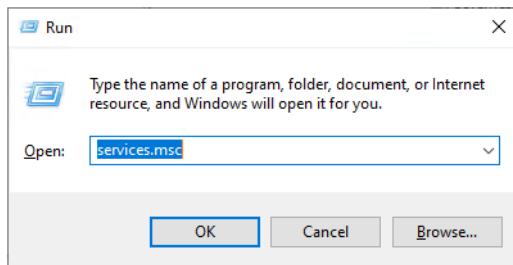
1. Follow [Step 2 to Step 12](#) to configure CoLA and the tunneling service.
2. Open a Command Prompt.
3. Update the CoLA server license port in the file `C:\Program Files\gemsLicenseServer\config\Cola_Config.txt`:
 - a. Edit the file using the Notepad editor.
 - b. Replace

```
LICENSE_PORT=17767
```

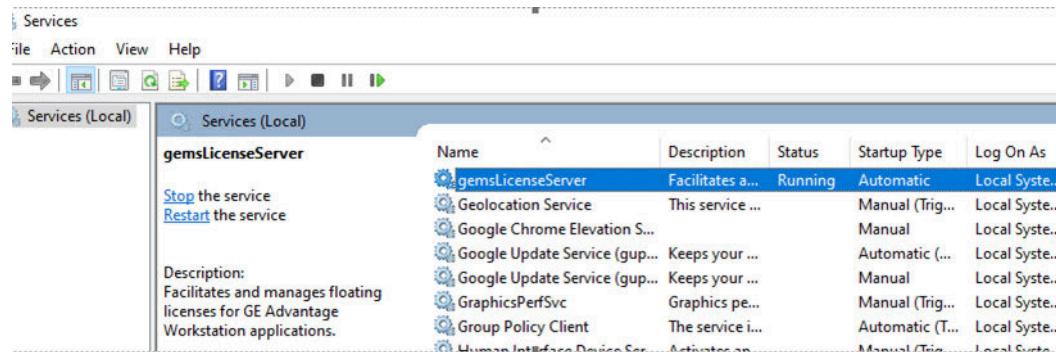
by

```
LICENSE_PORT=17768
```

4. Restart `gemsLicenseServer` Windows service or restart the system to apply port allocation:
 - a. Press **<Win> + <R>** to open the Run dialog.
 - b. Execute **services.msc** to open the Services window.



c. Right-click on **gemsLicenseServer** and select **Restart**.



5. Download the tunneling service package for Windows from <https://www.stunnel.org/downloads.html>.

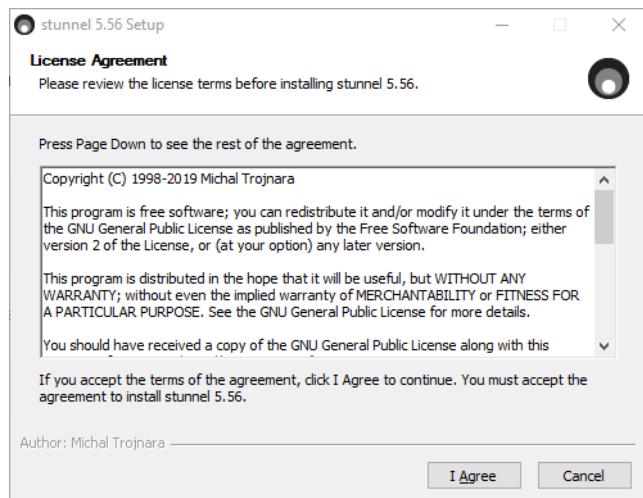


6. Install the **stunnel-5.56-win64-installer.exe** package:

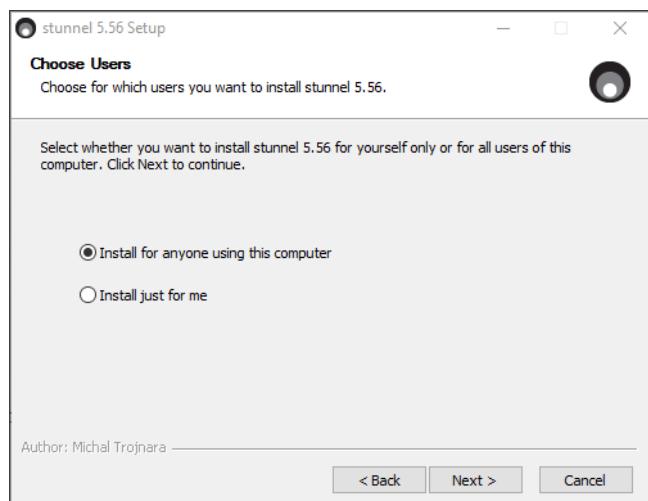
NOTE

If Openssl asks certificate relevant questions, add a dummy values as certificate is managed from the AW Server side.

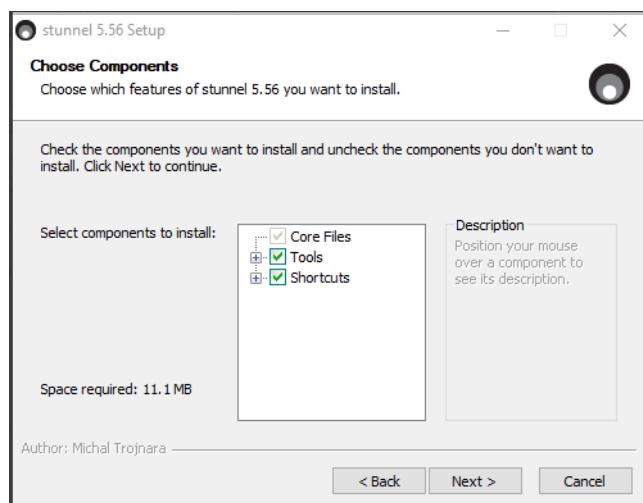
a. When the License Agreement appears, click on **I Agree**.



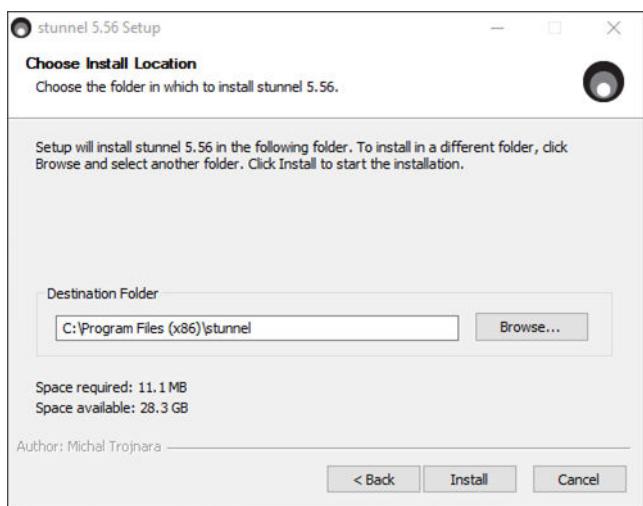
- b. On the *Choose Users* panel, keep selection and click on **Next**.



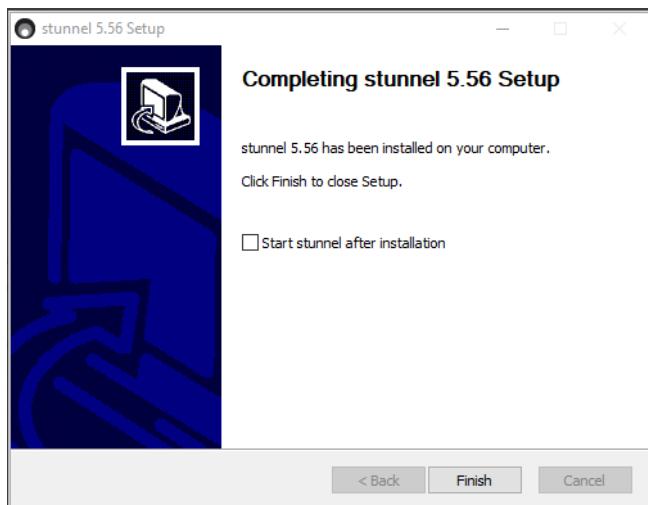
- c. On the *Choose Components* panel, keep selection and click on **Next**.



- d. On the *Choose Install Location* panel, keep destination folder and click on **Install**.



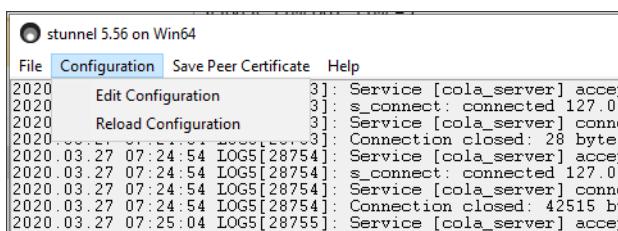
- e. When the installation is completed check **Start stunnel after installation** and click on **Finish**.



7. NOTE

This is an optional step - in case it is not done previously.
From the AW Server used as licensing client, where the certificate is generated, copy the file /etc/stunnel/cola.pem to C:\Program Files (x86)\stunnel\config using SCP or WinSCP.

8. From the stunnel user interface, edit the configuration file by selecting **Configuration > Edit Configuration**:



9. Update the SSL version in the configuration file:

Replace

```
sslVersion = ...
sslVersionMax = ...
```

by

```
sslVersionMax = TLSv1.2
sslVersion = TLSv1.2
```

10. Delete all lines related to client and server mode services:

```
***** Example TLS client mode services
```

and

```
***** Example TLS server mode services
```

11. Copy the following text and paste it at the end of the file:

```
[cola_server]
accept=17767
connect = 17768
cert = cola.pem
CAfile=cola.pem
verify=3
```

12. From the stunnel user interface, select **Configuration > Reload Configuration**.

In the stunnel user interface, at the bottom of the log, Configuration successful appears.

13. Follow [Step 14](#) to [Step 16](#) to configure the Apache server and revoke remote access.

It will restrict the local access in order to make the configuration of the licenses more secure.

14. Update the file C:\Program Files\gemsLicenseServer\Apache2\conf\httpd.conf:

- a. Edit the file using the Notepad editor as Administrator.
- b. Search for the following section:

```
<Directory "C:/PROGRA~1/gemsLicenseServer/Apache2/cgi-bin">
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>
```

- c. Replace

```
Allow from all
```

by

```
Allow from 127.0.0.1
```

15. Update the shortcut **FL Service Menu** on the Desktop of the user by replacing the URL

<http://<IP>:80/cgi-bin/smain.cgi> by <http://localhost/cgi-bin/smain.cgi>.

16. Restart the Apache Windows service or restart the system to apply the changes.

Proceed as described in [Step 4](#) (replacing the gemsLicenseServer Windows service by the Apache Windows service).

3.4.8.2.5 Fixing the CoLA License Server security vulnerability with the Apache UI on Windows

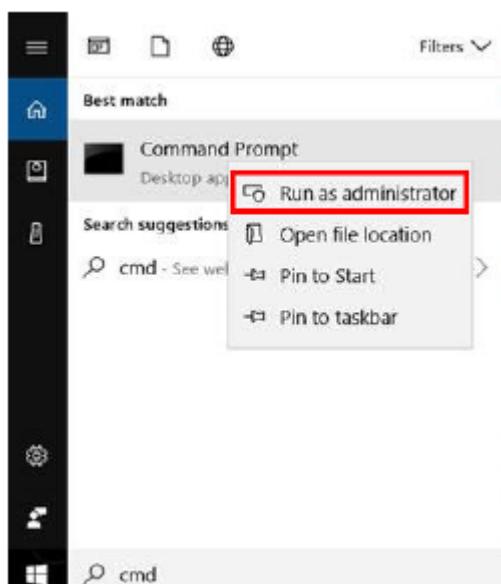
To fix the vulnerability with the Apache UI component on the CoLA 3.3.1 License Server installed on Windows, follow the below steps:

1. Block the Port 80 on the firewall.

By default the Apache is listening on this port, so with the Customer IT Admin's agreement and help, block the port 80 on the Windows firewall.

2. With the Customer IT Admin's agreement and help, execute a vulnerability scan.
3. If the report of the scan does not show the vulnerability anymore, stop the procedure here. Otherwise, follow the nexts steps to prevent this security vulnerability issue.
4. Access the Windows machine hosting the CoLA Licensing Server.
5. Login using administrator credential provided by the Customer IT Admin.
6. Delete the **FL Service Menu** desktop icon.
7. Open a Command Prompt as administrator.

From the Windows Search field type **cmd** then right-click on **Command Prompt** and select **Run as administrator**.



8. In the Command Prompt, change directory:

```
cd "%ProgramFiles%\gemsLicenseServer\Apache2\bin" <Enter>
```

9. Stop and uninstall the Apache server:

```
Apache.exe -k stop <Enter>
```

```
Apache.exe -k uninstall <Enter>
```

10. Verify that the Apache service is removed, using the following command:

```
services.msc <Enter>
```

The list of Services opens in a separate windows.

11. Verify that the Apache service is not present in the list (there is no Apache related name in the first column).

12. Close the Services window.

13. In the Command Prompt, delete the Apache folder:

```
cd <Enter>
rmdir /S /Q "%ProgramFiles%\gemsLicenseServer\Apache2" <Enter>
```

3.4.8.3 Security vulnerability in Apache's Log4J2 component

Problem: A Security vulnerability (CVE-2021-44228) has been found in the Apache's Log4J2 component which is commonly used in Java products for logging. The vulnerability might enable an attacker to execute arbitrary code on the AW server 3.2 Ext. 4.2.

Solution: To eliminate the threat, after the AW Server installation, disable the impacted services on the AW Server and remove the configuration that monitors the services at the HealthPage:

1. Open the AW Server Console/terminal, login as **root**.

2. Stop and disable the impacted services:

```
systemctl stop application-svc.service <Enter>
systemctl disable application-svc.service <Enter>
systemctl stop applist-svc.service <Enter>
systemctl disable applist-svc.service <Enter>
systemctl stop endofreview-svc.service <Enter>
systemctl disable endofreview-svc.service <Enter>
systemctl stop visualization-svc.service <Enter>
systemctl disable visualization-svc.service <Enter>
```

3. Navigate to the /var/lib/ServiceTools/conf directory:

```
cd /var/lib/ServiceTools/conf <Enter>
```

4. Backup the service-list.xml file:

```
cp service-list.xml service-list.xml.orig <Enter>
```

5. Remove the configuration that monitors the services at the HealthPage:

```
sed -e '/application-svc/,+39d' service-list.xml.orig > service-list.xml <Enter>
```

6. Reboot the AW Server by executing:

```
reboot <Enter>
```

7. Open again a Terminal tool on the AW Server, login as **root**.

8. Verify that all of the services are stopped by executing:

```
systemctl status application-svc.service <Enter>
systemctl status applist-svc.service <Enter>
systemctl status endofreview-svc.service <Enter>
systemctl status visualization-svc.service <Enter>
```

The result of each above command should contain the following line:

```
Active: inactive (dead)
```

3.4.8.4 SSL cypher security level too low

Problem: In AW Server 3.2 Ext. 4.0, the SSL cypher security level is too low. Even if it does not violate the specification for this version, the SSL cypher security level should be at least higher than on previous AW Server releases.

Solution: To increase the SSL cypher security level, update the SSL setting to have a stronger configuration:

1. Put the AW Server in maintenance mode, to guarantee there is no user connected to the AW Server, as an Apache restart will be necessary.
2. Open the AW Server Console/terminal, login as **root**.
3. Navigate to the /etc/httpd/conf.d directory:

```
cd /etc/httpd/conf.d <Enter>
```

4. Backup the ssl.conf file:

```
cp ssl.conf ssl.conf.orig <Enter>
```

5. Update the ssl.conf file:

```
sed -i 's/^SSLCipherSuite.*$/  
SSLCipherSuite ECDHE-RSA-AES128-SHA256:HIGH:!aNULL:!MD5:!3DES:  
DHE-RSA-AES128-SHA:!DHE-RSA-AES128-SH256:!DHE-RSA-AES256-SHA:!DHE-RSA-  
AES256-SHA256:!DHE-RSA-CAMELLIA128-SHA:!DHE-RSA-CAMELLIA256-SHA:!ECDHE-  
RSA-AES128-SHA:!ECDHE-RSA-AES128-SHA256:!ECDHE-RSA-AES256-SHA:!ECDHE-  
RSA-AES256-SHA384:!AES128-SHA:!AES128-SHA256:!AES128-GCM-SHA256:!AES256-  
SHA:!AES256-SHA256:!AES256-GCM-SHA384:!CAMELLIA128-SHA:!CAMELLIA256-  
SHA:!DHE-RSA-AES128-SHA256/g' ssl.conf <Enter>
```

NOTE

Copy the first line then append the other lines one by one (without blank space), as it should appear on one line in the file.

6. Verify that the ssl.conf file is updated correctly:

```
diff ssl.conf ssl.conf.orig <Enter>
```

The following lines appear:

```
< SSLCipherSuite ECDHE-RSA-AES128-SHA256:HIGH:!aNULL:!MD5:!3DES:  
DHE-RSA-AES128-SHA:!DHE-RSA-AES128-SH256:!DHE-RSA-AES256-SHA:!DHE-RSA-  
AES256-SHA256:!DHE-RSA-CAMELLIA128-SHA:!DHE-RSA-CAMELLIA256-SHA:!ECDHE-  
RSA-AES128-SHA:!ECDHE-RSA-AES128-SHA256:!ECDHE-RSA-AES256-SHA:!ECDHE-  
RSA-AES256-SHA384:!AES128-SHA:!AES128-SHA256:!AES128-GCM-SHA256:!AES256-  
SHA:!AES256-SHA256:!AES256-GCM-SHA384:!CAMELLIA128-SHA:!CAMELLIA256-  
SHA:!DHE-RSA-AES128-SHA256
```

```
---
```

```
> SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
```

7. Restart the Apache service:

```
systemctl restart httpd <Enter>
```

8. Exit the maintenance mode.

3.5 HPE ProLiant DL360 Gen10 Server hardware troubleshooting

NOTICE

The information in this section applies primarily to GE-supplied hardware. For sites at which AW Server platform software (in virtualized mode) is or will be installed on customer-supplied hardware, this information should be used as a guideline and adapted accordingly; refer also to customer site IT policies and procedures.

For more details on this section, refer to the HPE ProLiant DL360 Gen10 Server 869839-404 and follow instructions of section "Component identification".

NOTICE

The HPE ProLiant DL360 Gen10 Server 869839-404 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.5.1 HPE ProLiant DL360 Gen10 Server mechanical components description

Refer to section "Mechanical components" in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404, for an illustrated view of the mechanical components.

NOTE

Parts illustrated in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404 are not GEHC FRUS (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

3.5.2 HPE ProLiant DL360 Gen10 Server system components description

Refer to section "System components" in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404 for an illustrated view of the system components.

NOTE

Parts illustrated in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404 are not GEHC FRUS (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

3.5.3 HPE ProLiant DL360 Gen10 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.5.3.1 HPE ProLiant DL360 Gen10 Server front panel LEDs codes

Refer to section "Front panel LEDs and buttons" in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404.

3.5.3.2 HPE ProLiant DL360 Gen10 Server Systems Insight Display LEDs codes

Refer to section "Systems Insight Display LEDs" in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404.

3.5.3.3 HPE ProLiant DL360 Gen10 Server hard disk drives LEDs codes

Refer to section "Hard disk drives LEDs codes" in the HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404.

3.5.4 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.5.5 HPE ProLiant DL360 Gen10 Server troubleshooting tips

Before contacting the HPE support center for any related issue, you should try to identify more precisely the failing hardware piece.

- Open the Terminal tool and run the **sosreport** command (`/usr/sbin/sosreport`). This command is included in the Operating System and will build a tar file with the system information that is used by Linux support engineers, in order to diagnose problems.

The output log file is created in `/tmp` directory.

Following the HPE ProLiant DL360 Gen10 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

| Device | Instructions / Linux Command | Parameters |
|----------------------|--|---|
| Information | sosreport | System hardware information |
| Internal controller | /usr/sbin/ssacli controller slot=0 show | Battery/capacitor status
Controller status |
| Internal disk status | /usr/sbin/ssacli controller slot=0 logicaldrive all show | Internal logical drive status |
| Internal disk status | /usr/sbin/ssacli controller slot=0 physicaldrive all show | Individual physical drive status |

| Device | Instructions / Linux Command | Parameters |
|-----------------------------------|---|--|
| Internal server
sea of sensors | <pre>ipmitool sensor egrep 'RPM degrees Volts Watts Fan'</pre> <p>NOTE</p> <ul style="list-style-type: none"> The PowerMeter info shall not be taken into account. The status of Power supplies and Fans is nc by default. The status of temperature sensors is na by default | Power supplies status
Fans status
Temperature sensors status |

NOTE

On some AW Server (prior to AW Server 3.2 Ext. 4.0), the **ssacli** utility is not embedded in the AW Server package and should be installed as described in [3.4.6.12 Hard drives check command not working on HPE ProLiant DL360 Gen9 Server on page 227](#).

3.5.6 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the **70-persistent-net.rules** file with the the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
3. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.5.7 Network Card 10Gb/s and virtual switch interaction

NOTICE

Do not use the 10Gb/s port with a virtual NIC switch supporting 10Gb/s. Indeed, in such case the switch is not seeing the correct MAC address.In this case, permanent MAC address shall be used

NOTE

If you encounter this situation, please refer to the site's IT admin to change the switch behavior.

3.6 HPE ProLiant DL360 Gen9 Server hardware troubleshooting

NOTICE

The information in this section applies primarily to GE-supplied hardware. For sites at which AW Server platform software (in virtualized mode) is or will be installed on customer-supplied hardware, this information should be used as a guideline and adapted accordingly; refer also to customer site IT policies and procedures.

For more details on this section, refer to the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 and follow instructions of section "Component identification".

NOTICE

The HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.6.1 HPE ProLiant DL360 Gen9 Server mechanical components description

Refer to section "Mechanical components" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 for an illustrated view of the mechanical components.

NOTE

Parts illustrated in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 are not GEHC FRUS (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

3.6.2 HPE ProLiant DL360 Gen9 Server system components description

Refer to section "System components" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 for an illustrated view of the system components.

NOTE

Parts illustrated in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 are not GEHC FRUS (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

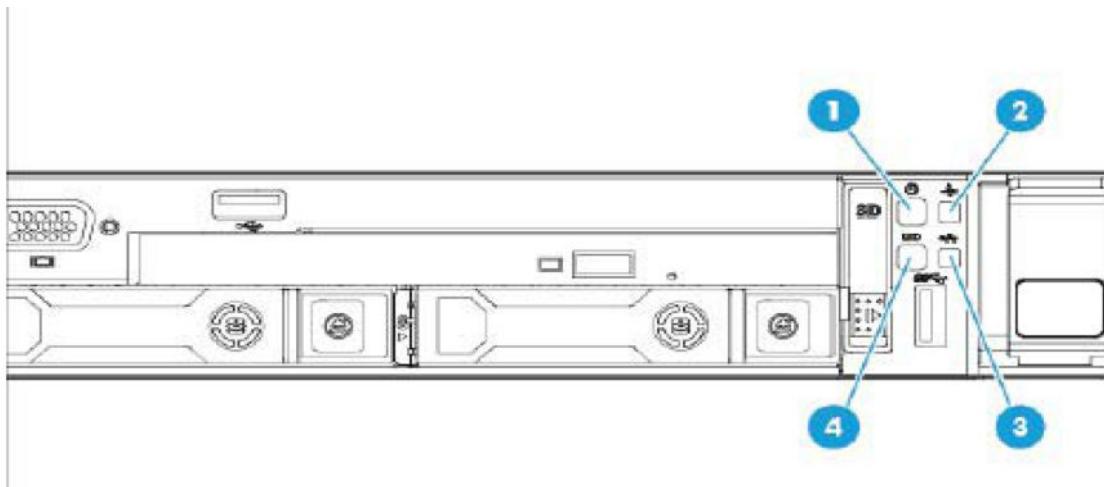
3.6.3 HPE ProLiant DL360 Gen9 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.6.3.1 HPE ProLiant DL360 Gen9 Server front panel LEDs codes

Refer to section "Front panel LEDs and buttons" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.



| Item | Description | Status |
|------|---|---|
| 1 | Power On/Standby button and system power LED* | Solid green = System on
Flashing green (1 Hz/cycle per sec) = Performing power on sequence
Solid amber = System in standby
Off = No power present** |
| 2 | Health LED* | Solid green = Normal
Flashing green (1 Hz/cycle per sec) = iLO is rebooting.
Flashing amber = System degraded
Flashing red (1 Hz/cycle per sec) = System critical† |
| 3 | NIC status LED* | Solid green = Link to network
Flashing green (1 Hz/cycle per sec) = Network active
Off = No network activity |
| 4 | UID button/LED* | Solid blue = Activated
Flashing blue: <ul style="list-style-type: none"> • 1 Hz/cycle per sec = Remote management or firmware upgrade in progress • 4 Hz/cycle per sec = iLO manual reboot sequence initiated • 8 Hz/cycle per sec = iLO manual reboot sequence in progress Off = Deactivated |

*When all four LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see "Power fault LEDs."

**Facility power is not present, power cord is not attached, no power supplies are installed, power supply failure has occurred, or the power button cable is disconnected.

†If the health LED indicates a degraded or critical state, review the system IML or use iLO to review the system health status.

3.6.3.2 HPE ProLiant DL360 Gen9 Server Systems Insight Display LEDs codes

Power fault LEDs

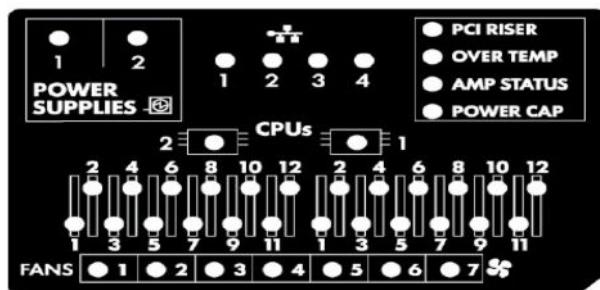
The following table provides a list of power fault LEDs, and the subsystems that are affected. Not all power faults are used by all servers.

Refer to section "Systems Insight Display LEDs" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.

| Subsystem | LED behavior |
|---|--------------|
| System board | 1 flash |
| Processor | 2 flashes |
| Memory | 3 flashes |
| Riser board PCIe slots | 4 flashes |
| FlexibleLOM | 5 flashes |
| Removable HP Flexible Smart Array controller/Smart SAS HBA controller | 6 flashes |
| System board PCIe slots | 7 flashes |
| Power backplane or storage backplane | 8 flashes |
| Power supply | 9 flashes |

Systems Insight Display LEDs

The Systems Insight Display LEDs represent the system board layout. The display provides status for all internal LEDs and enables diagnosis with the access panel installed. To view the LEDs, access the Systems Insight Display.

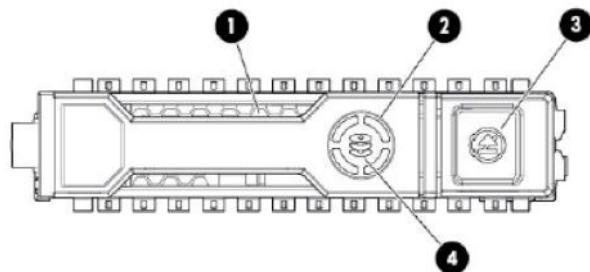


| Description | Status |
|----------------|--|
| Processor LEDs | Off = Normal
Amber = Failed processor |
| DIMM LEDs | Off = Normal
Amber = Failed DIMM or configuration issue |
| Fan LEDs | Off = Normal
Amber = Failed fan or missing fan |
| NIC LEDs | Off = No link to network
Solid green = Network link
Flashing green = Network link with activity
If power is off, the front panel LED is not active. For status, see "Rear panel LEDS and buttons (on page 84)." |

| Description | Status |
|-------------------|--|
| Power supply LEDs | Off = Normal
Amber = Failed power supply |
| PCI riser LED | Off = Normal
Amber = Incorrectly installed PCI riser cage |
| Over temp LED | Off = Normal
Amber = High system temperature detected |
| Amp Status LED | Off = AMP modes disabled
Solid green = AMP mode enabled
Solid amber = Failover
Flashing amber = Invalid configuration |
| Power cap LED | Off = System is in standby, or no cap is set.
Solid green = Power cap applied |

3.6.3.3 HPE ProLiant DL360 Gen9 Server hard disk drives LEDs codes

Refer to section "Hot-plug drive LED definitions" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.

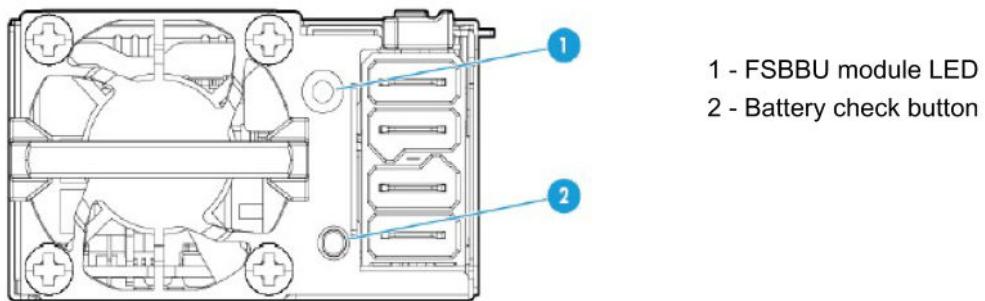


| Item | LED | Status | Definition |
|------|---------------|----------------------|--|
| 1 | Locate | Solid blue | The drive is being identified by a host application. |
| | | Flashing blue | The drive carrier firmware is being updated or requires an update. |
| 2 | Activity ring | Rotating green | Drive activity |
| | | Off | No drive activity |
| 3 | Do not remove | Solid white | Do not remove the drive. Removing the drive causes one or more of the logical drives to fail. |
| | | Off | Removing the drive does not cause a logical drive to fail. |
| 4 | Drive status | Solid green | The drive is a member of one or more logical drives. |
| | | Flashing green | The drive is rebuilding or performing a RAID migration, strip size migration, capacity expansion, or logical drive extension, or is erasing. |
| | | Flashing amber/green | The drive is a member of one or more logical drives and predicts the drive will fail. |
| | | Flashing amber | The drive is not configured and predicts the drive will fail. |
| | | Solid amber | The drive has failed. |
| | | Off | The drive is not configured by a RAID controller. |

3.6.3.4 HPE ProLiant DL360 Gen9 Server flex slot battery backup module LEDs and buttons

When the battery check button is pressed, the LED indicates the state of the battery. The number of times that the LED flashes indicates the state of change.

Refer to section "Flex slot battery backup module LEDs and buttons" in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.



| # of LED flashes | % state of change |
|------------------|-------------------|
| 0 | < 5% |
| 1 | <= 30% |
| 2 | 31% – 69% |
| 3 | >= 70% |

The state of the LED indicates the FSBBU operating mode.

| LED | Mode/State |
|----------------|---|
| Off | <ul style="list-style-type: none"> Ship/storage mode Cycle power operating |
| Flashing amber | <ul style="list-style-type: none"> Battery diagnostic Active mode |
| Solid amber | Online mode and charger is ON |
| Flashing green | <p>Discharge mode</p> <ul style="list-style-type: none"> RSOC—70-100% frequency=0.5Hz; duty=0.5 RSOC—31-69% frequency=1Hz; duty=0.5 RSOC—0-30% frequency=1.5Hz; duty=0.5 |
| Solid green | <ul style="list-style-type: none"> Online mode and charger is OFF Battery is fully charged |
| Flashing red | Auxiliary path A/B protection |

3.6.4 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.6.5 HPE ProLiant DL360 Gen9 Server troubleshooting tips

Before contacting the HPE support center for any related issue, you should try to identify more precisely the failing hardware piece.

- Open the Terminal tool and run the **sosreport** command (`/usr/bin/sosreport`). This command is included in the Operating System and will build a tar file with the system information that is used by Linux support engineers, in order to diagnose problems.

The output log file is created in `/tmp` directory.

Following the HPE ProLiant DL360 Gen9 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

NOTE

Use either the **ssacli** command or the **hpssacli** command. The commands displayed below use **ssacli**. If **ssacli** is not available, replace it by **hpssacli**.

| Device | Instructions / Linux Command | Parameters |
|--------------------------------|---|--|
| Information | sosreport | System hardware information |
| Internal controller | <code>/usr/sbin/ssacli controller slot=0 show</code> | Battery/capacitor status
Controller status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 logicaldrive all show</code> | Internal logical drive status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 physicaldrive all show</code> | Individual physical drive status |
| Internal server sea of sensors | ipmitool sensor egrep 'RPM degrees Volts Watts Fan'
NOTE <ul style="list-style-type: none"> • The PowerMeter info shall not be taken into account. • The status of Power supplies and Fans is nc by default. • The status of temperature sensors is na by default | Power supplies status
Fans status
Temperature sensors status |

3.6.6 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the `70-persistent-net.rules` file with the the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
3. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.6.7 Network Card 10Gb/s and virtual switch interaction

NOTICE

Do not use the 10Gb/s port with a virtual NIC switch supporting 10Gb/s. Indeed, in such case the switch is not seeing the correct MAC address. In this case, permanent MAC address shall be used

NOTE

If you encounter this situation, please refer to the site's IT admin to change the switch behavior.

3.6.8 Smart Array P440ar Controller setup error

Problem: During the BIOS parameters setup for the HPE ProLiant DL360 Gen9 Server, when trying to open the Smart Array P440ar Controller setup menu, a pop up messages displays mentioning that the controller contains a logical drive that was created with a newer version of the Array Configuration tools.

Refer to the AW Server 3.2 Hardware Installation Manual, Job Card IST005 - HPE ProLiant DL360 Gen9 Server Installation Steps.

Solution: Update the Smart Array Controller firmware to the latest version as described below:

1. From your laptop, download the Smart Array Controller firmware RPM package from the HPE support site, and copy it on an USB device:

https://support.hpe.com/hpsc/swd/public/detail?sp4ts.oid=7274897&swItemld=MTX_cd2e7cc9f677434ca79b0faf43&swEnvOid=4184#tab3

2. At the KVM or from the iLO login as **root**.

3. Start the graphical environment:

startx <Enter>

4. Copy the package on the desktop from the USB device.

5. Open a Terminal window and navigate to the desktop folder:

cd Desktop <Enter>

6. List the content of the desktop:

ls <Enter>

You should see the RPM filename (*<rpm_filename>*) similar to the following filename (the version may vary):

firmware-smartarray-ea3138d8e8-6.60-2.1.x86_64.rpm

7. Extract the contents of the RPM using the command:

```
rpm2cpio <rpm_filename> | cpio -id <Enter>
```

This extracts the contents of the RPM to 'usr' folder in the current folder.

8. Navigate to the following folder:

```
cd /usr/lib/x86_64-linux-gnu/firmware-smartarray-ea3138d8e8-* <Enter>
```

9. Run the following command to update the firmware (if you are prompted to select which device to flash, select (A)ll):

```
./setup <Enter>
```

10. Reboot the system:

```
reboot <Enter>
```

The Smart Array Controller firmware is now updated to the latest version.

3.7 HPE ProLiant DL560 Gen8 Server hardware troubleshooting

NOTICE

The information in this section applies primarily to GE-supplied hardware. For sites at which AW Server platform software (in virtualized mode) is or will be installed on customer-supplied hardware, this information should be used as a guideline and adapted accordingly; refer also to customer site IT policies and procedures.

For more details on this section, refer to the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005, and follow instructions of section "Component identification".

NOTICE

The HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.7.1 HPE ProLiant DL560 Gen8 Server mechanical components description

Refer to section "Mechanical Components" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005 for an illustrated view of the mechanical components.

NOTE

Parts illustrated in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005 are not GEHC FRUs (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

3.7.2 HPE ProLiant DL560 Gen8 Server system components description

Refer to section "System components" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005 for an illustrated view of the mechanical components.

NOTE

Parts illustrated in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005 are not GEHC FRUS (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

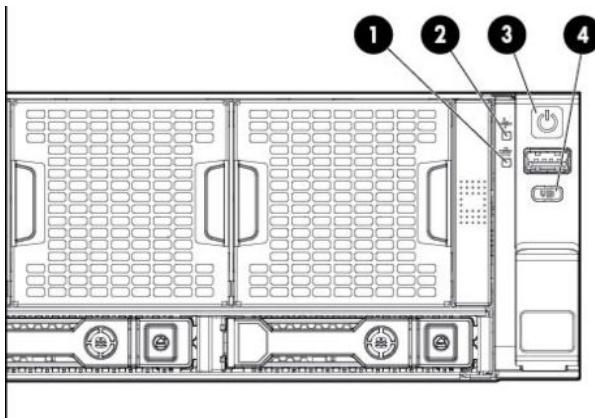
3.7.3 HPE ProLiant DL560 Gen8 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.7.3.1 HPE ProLiant DL560 Gen8 Server front panel LEDs codes

Refer to section "Front panel LEDs and buttons" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005.



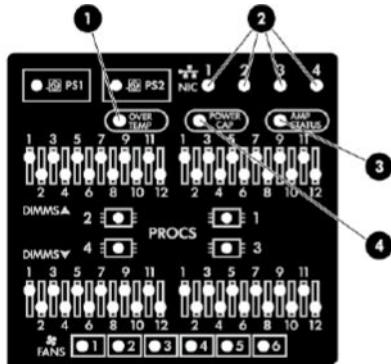
| Item | Description | Status |
|------|--|---|
| 1 | NIC status LED | Solid green = Link to network
Flashing green (1 Hz/cycle per sec) = Network active
Off = No network activity |
| 2 | Health LED | Solid green = Normal
Flashing amber = System degraded
Flashing red (1 Hz/cycle per sec) = System critical
Fast-flashing red (4 Hz/cycles per sec) = Power fault* |
| 3 | Power On/Standby button and system power LED | Solid green = System on
Flashing green (1 Hz/cycle per sec) = Performing power on sequence
Solid amber = System in standby
Off = No power present** |
| 4 | UID button/LED | Solid blue = Activated
Flashing blue (1 Hz/cycle per sec) = Remote management or firmware upgrade in progress
Off = Deactivated |

* To identify components in a degraded or critical state, see the Systems Insight Display LEDs, check iLO/BIOS logs, and reference the server troubleshooting guide.

** Facility power is not present, power cord is not attached, no power supplies are installed, power supply failure has occurred, or the power button cable is disconnected.

3.7.3.2 HPE ProLiant DL560 Gen8 Server Systems Insight Display LEDs codes

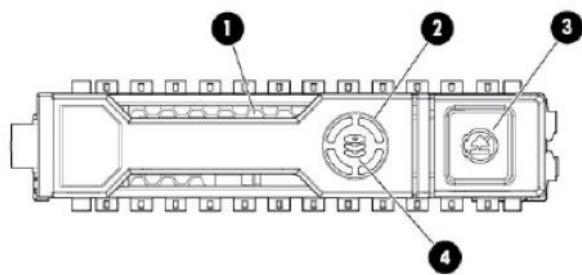
Refer to section "Systems Insight Display LEDs" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005.



| Item | Description | Status |
|------|-------------------|--|
| 1 | Over temp | Off = Normal
Solid amber = High system temperature detected |
| 2 | NIC link/activity | Off = No link to network. If the power is off, view the rear panel RJ-45 LEDs for status ("Rear panel LEDs and buttons" on page 73).
Flashing green = Network link and activity
Solid green = Network link |
| 3 | AMP status | Off = AMP modes disabled
Solid green = AMP mode enabled
Solid amber = Failover
Flashing amber = Invalid configuration |
| 4 | Power cap | Off = System is in standby, or no cap is set.
Solid green = Power cap applied |
| — | All other LEDs | Off = Normal
Amber = Failure
For more information on the activation of these LEDs, see "Systems Insight Display LED combinations (on page 71)." |

3.7.3.3 HPE ProLiant DL560 Gen8 Server hard disk drives LEDs codes

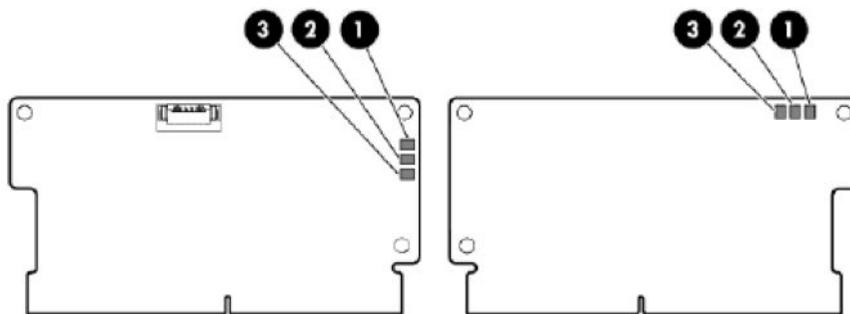
Refer to section "Hot-plug drive LED definitions" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005.



| Item | LED | Status | Definition |
|------|---------------|----------------------|--|
| 1 | Locate | Solid blue | The drive is being identified by a host application. |
| | | Flashing blue | The drive carrier firmware is being updated or requires an update. |
| 2 | Activity ring | Rotating green | Drive activity |
| | | Off | No drive activity |
| 3 | Do not remove | Solid white | Do not remove the drive. Removing the drive causes one or more of the logical drives to fail. |
| | | Off | Removing the drive does not cause a logical drive to fail. |
| 4 | Drive status | Solid green | The drive is a member of one or more logical drives. |
| | | Flashing green | The drive is rebuilding or performing a RAID migration, strip size migration, capacity expansion, or logical drive extension, or is erasing. |
| | | Flashing amber/green | The drive is a member of one or more logical drives and predicts the drive will fail. |
| | Drive status | Flashing amber | The drive is not configured and predicts the drive will fail. |
| | | Solid amber | The drive has failed. |
| | | Off | The drive is not configured by a RAID controller. |

3.7.3.4 HPE ProLiant DL560 Gen8 Server FBWC module LEDs codes

The Flash Backed Write Cache (FBWC) module has three single-color LEDs (one amber and two green). The LEDs are duplicated on the reverse side of the cache module to facilitate status viewing. Refer to section "FBWC module LEDs (P222, P420, P421)" in the HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005.



| 1 - Amber | 2 - Green | 3 - Green | Interpretation |
|---------------|-----------------|-----------------|---|
| Off | Off | Off | The cache module is not powered. |
| Off | Flashing 0.5 Hz | Flashing 0.5 Hz | The cache microcontroller is executing from within its boot loader and receiving new flash code from the host controller. |
| Off | Flashing 1 Hz | Flashing 1 Hz | The cache module is powering up, and the capacitor pack is charging. |
| Off | Off | Flashing 1 Hz | The cache module is idle, and the capacitor pack is charging. |
| Off | Off | On | The cache module is idle, and the capacitor pack is charged. |
| Off | On | On | The cache module is idle, the capacitor pack is charged, and the cache contains data that has not yet been written to the drives. |
| Off | Flashing 1 Hz | Off | A backup is in progress. |
| Off | On | Off | The current backup is complete with no errors. |
| Flashing 1 Hz | Flashing 1 Hz | Off | The current backup failed, and data has been lost. |
| Flashing 1 Hz | Flashing 1 Hz | On | A power error occurred during the previous or current boot. Data may be corrupt. |
| Flashing 1 Hz | On | Off | An overtemperature condition exists. |
| Flashing 2 Hz | Flashing 2 Hz | Off | The capacitor pack is not attached. |
| Flashing 2 Hz | Flashing 2 Hz | On | The capacitor has been charging for 10 minutes, but has not reached sufficient charge to perform a full backup. |
| On | On | Off | The current backup is complete, but power fluctuations occurred during the backup. |
| On | On | On | The cache module microcontroller has failed. |

3.7.4 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.7.5 HPE ProLiant DL560 Gen8 Server troubleshooting tips

Before contacting the HPE support center for any related issue, you should try to identify more precisely the failing hardware piece.

- Open the Terminal tool and run the **sosreport** command (`/usr/sbin/sosreport`). This command is included in the Operating System and will build a tar file with the system information that is used by Linux support engineers, in order to diagnose problems.

The output log is created in `/tmp` directory.

Following the HPE ProLiant DL560 Gen8 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

NOTE

Use either the **ssacli** command or the **hpssacli** command. The commands displayed below use **ssacli**. If **ssacli** is not available, replace it by **hpssacli**.

| Device | Instructions / Linux Command | Parameters |
|--------------------------------|--|--|
| Information | sosreport | System hardware information |
| Internal controller | <code>/usr/sbin/ssacli controller slot=0 show</code> | Battery/capacitor status
Controller status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 logicaldrive all show</code> | Internal logical drive status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 physicaldrive all show</code> | Individual physical drive status |
| DAS status | <code>/usr/sbin/ssacli controller slot=2 physicaldrive all show</code> | DAS drive status |
| Internal server sea of sensors | ipmitool sensor egrep 'RPM degrees Volts Watts Fan'
NOTE <ul style="list-style-type: none"> • The PowerMeter info shall not be taken into account. • The status of Power supplies and Fans is nc by default. • The status of temperature sensors is na by default. | Power supplies status
Fans status
Temperature sensors status |

3.7.6 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the `70-persistent-net.rules` file with the the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
3. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.8 HPE ProLiant DL580 G7 Server hardware troubleshooting

NOTICE

The information in this section applies primarily to GE-supplied hardware. For sites at which AW Server platform software (in virtualized mode) is or will be installed on customer-supplied hardware, this information should be used as a guideline and adapted accordingly; refer also to customer site IT policies and procedures.

For more details on this section, refer to the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005, and follow instructions of section "Component identification".

NOTICE

The HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.8.1 HPE ProLiant DL580 G7 Server mechanical components description

Refer to section "Mechanical components" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005 for an illustrated view of the mechanical components.

NOTE

Parts illustrated in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005 are not GEHC FRUs (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

3.8.2 HPE ProLiant DL580 G7 Server system components description

Refer to section "System components" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005 for an illustrated view of the system components.

NOTE

Parts illustrated in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005 are not GEHC FRUs (Field replaceable Units). HPE is fully responsible for servicing the hardware and replacing hardware components.

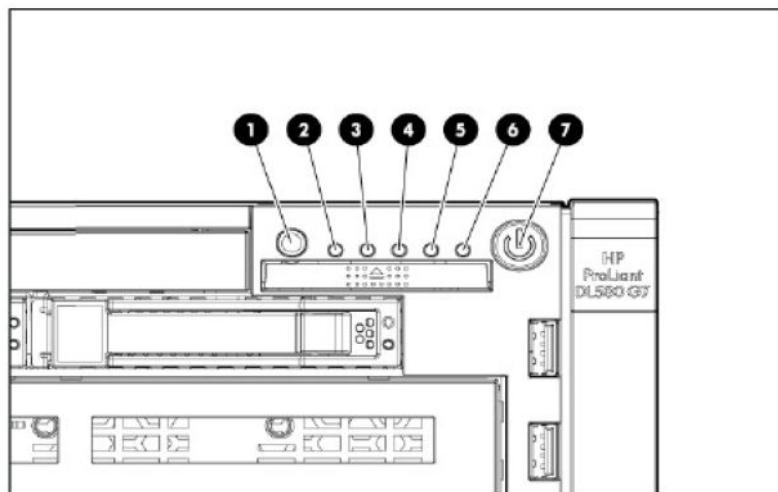
3.8.3 HPE ProLiant DL580 G7 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.8.3.1 HPE ProLiant DL580 G7 Server front panel LEDs code meaning

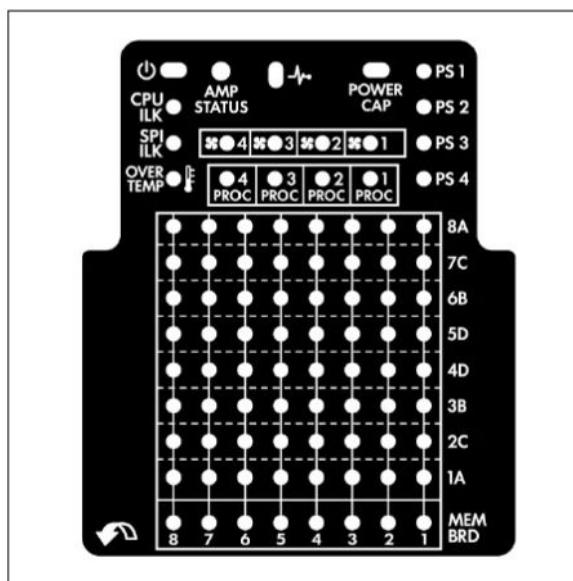
Refer to section "Front panel LEDs and buttons" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005.



| Item | Description | Status |
|------|---------------------------------|---|
| 1 | UID button and LED | Blue—Activated
Blue (flashing)—Server being managed remotely
Off—Deactivated |
| 2 | Health LED | Green—Normal (system on)
Amber (flashing)—Internal system health degraded
Red (flashing)—Internal system health critical
Off—Normal (system off) |
| 3 | NIC 1 LED | Green—Linked to network
Green (flashing)—Linked with activity on the network
Off—No network connection |
| 4 | NIC 2 LED | Green—Linked to network
Green (flashing)—Linked with activity on the network
Off—No network connection |
| 5 | NIC 3 LED | Green—Linked to network
Green (flashing)—Linked with activity on the network
Off—No network connection |
| 6 | NIC 4 LED | Green—Linked to network
Green (flashing)—Linked with activity on the network
Off—No network connection |
| 7 | Power on/Standby button and LED | Amber—System has AC power and is in standby mode.
Green—System has AC power and is powered on.
Off—System has no AC power. |

3.8.3.2 HPE ProLiant DL580 G7 Server Systems Insight Display LEDs

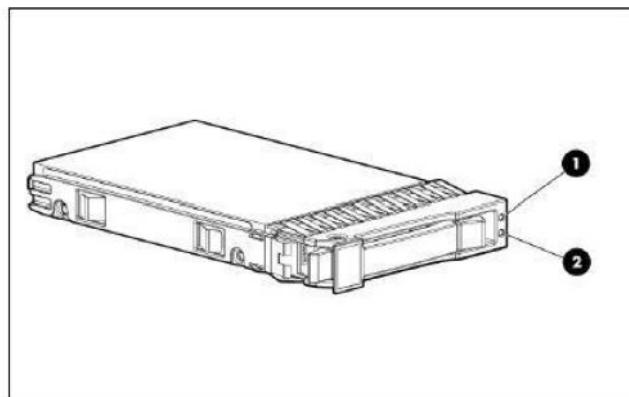
Refer to section "Systems Insight Display" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005.



| LED | Description |
|----------------|---|
| AMP status | Off—No protection
Green—Protection enabled
Amber—Memory failure occurred
Amber (flashing)—Memory configuration error |
| Health | Green—Normal (system on)
Amber (flashing)—Internal system health degraded
Red (flashing)—Internal system health critical
Off—Normal (system off) |
| Power cap | Green—System on or requesting power on
Flashing amber—Power on denied
Off—Standby |
| All other LEDs | Off—Normal
Amber—Failed or missing component |

3.8.3.3 HPE ProLiant DL580 G7 Server SAS or SATA hard drive LED combinations

Refer to sections "Hard drive LEDs" and "Hard drive LED combinations" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005.



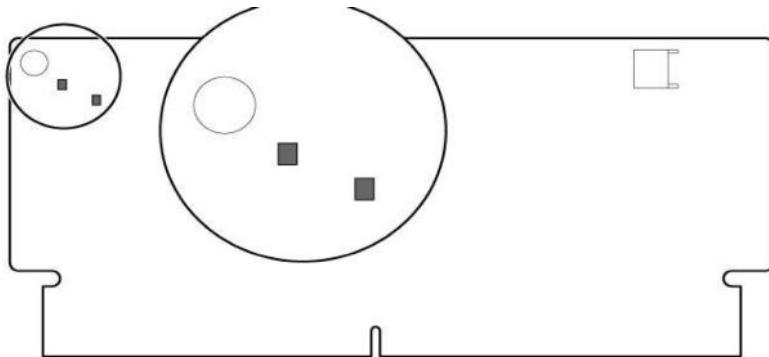
| Online/activity LED (green) | Fault/UID LED (amber/blue) | Interpretation |
|-----------------------------|----------------------------------|--|
| On, off, or flashing | Alternating amber and blue | The drive has failed, or a predictive failure alert has been received for this drive; it also has been selected by a management application. |
| On, off, or flashing | Steadily blue | The drive is operating normally, and it has been selected by a management application. |
| On | Amber, flashing regularly (1 Hz) | A predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| On | Off | The drive is online, but it is not active currently. |
| Flashing regularly (1 Hz) | Amber, flashing regularly (1 Hz) | Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.
The drive is part of an array that is undergoing capacity expansion or stripe migration, but a predictive failure alert has been received for this drive. To minimize the risk of data loss, do not replace the drive until the expansion or migration is complete. |
| Flashing regularly (1 Hz) | Off | Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.
The drive is rebuilding, erasing, or it is part of an array that is undergoing capacity expansion or stripe migration. |
| Flashing irregularly | Amber, flashing regularly (1 Hz) | The drive is active, but a predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| Flashing irregularly | Off | The drive is active, and it is operating normally. |
| Off | Steadily amber | A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible. |
| Off | Amber, flashing regularly (1 Hz) | A predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| Off | Off | The drive is offline, a spare, or not configured as part of an array. |

3.8.3.4 HPE ProLiant DL580 G7 Server FBWC RAID module LEDs code meaning

The Flash Backed Write Cache (FBWC) feature has two modules:

- The FBWC Cache module
- The FBWC capacitor pack

The FBWC Cache module has two single-color LEDs (green and amber). The LEDs are duplicated on the reverse side of the cache module to facilitate status viewing.



Green LED and Amber LED Interpretation

| Green LED | Amber LED | Interpretation |
|------------------|------------------|--|
| Off | On | A backup is in progress. |
| Flashing (1Hz) | On | A restore is in progress. |
| Flashing (1Hz) | Off | The capacitor pack is charging. |
| On | Off | The capacitor pack has completed charging. |

The capacitor pack may need to be replaced for LED status below:

| Green LED | Amber LED | Interpretation |
|---|---|--|
| Flashing (2Hz) . Alternating with amber LED | Flashing (2Hz) . Alternating with green LED | One of the following conditions exists: <ul style="list-style-type: none"> The charging process has timed out The capacitor pack is not connected. |

The Cache module is to be replaced for LED status below:

| Green LED | Amber LED | Interpretation |
|------------------|------------------|-------------------------------------|
| On | On | The flash code image failed to load |
| On | Off | The flash code is corrupt |

Refer to section "FBWC module LEDs" in the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005.

3.8.4 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.8.5 HPE ProLiant DL580 G7 Server troubleshooting tips

Before contacting the HPE support center for any related issue, you should try to identify more precisely the failing hardware piece.

- Open the Terminal tool and run the **sosreport** command (`/usr/sbin/sosreport`). This command is included in the Linux OS and will build a tar file with the system information that is used by Linux support engineers, in order to diagnose problems.

The output log file is created in `/var/log` directory.

Following the HPE ProLiant DL580 G7 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

NOTE

Use either the **ssacli** command or the **hpssacli** command. The commands displayed below use **ssacli**. If **ssacli** is not available, replace it by **hpssacli**.

| Device | Instructions / Linux Command | Parameters |
|--------------------------------|--|--|
| Information | sosreport | System hardware information |
| Internal controller | /usr/sbin/ssacli controller slot=0 show | Battery/capacitor status
Controller status |
| Internal disk status | /usr/sbin/ssacli controller slot=0 logicaldrive all show | Internal logical drive status |
| Internal disk status | /usr/sbin/ssacli controller slot=0 physicaldrive all show | Individual physical drive status |
| DAS status | /usr/sbin/ssacli controller slot=7 physicaldrive all show | DAS drive status |
| Internal server sea of sensors | ipmitool sensor egrep 'RPM degrees Volts Watts Fan'
NOTE <ul style="list-style-type: none"> • The PowerMeter info shall not be taken into account. • The status of Power supplies and Fans is nc by default. • The status of temperature sensors is na by default. | Power supplies status
Fans status
Temperature sensors status |

3.8.6 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the `70-persistent-net.rules` file with the the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
3. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:

- a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.9 HPE ProLiant ML350p Gen8 Server hardware troubleshooting

For more details on this section, refer to the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009, and follow instructions of section "Component identification".

NOTICE

The HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.9.1 HPE ProLiant ML350p Gen8 Server mechanical components description

Refer to section "Mechanical components" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 for an illustrated view of the mechanical components.

NOTE

All parts illustrated in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 are not FRUs (Field replaceable Units). Refer to the AW Server 3.2 Installation and Service Manual, HPE ProLiant ML350p Gen8 Server Low Tier – Hardware FRU's for information about the mechanical parts that are stored as FRU at GEHC warehouses.

3.9.2 HPE ProLiant ML350p Gen8 Server system components description

Refer to section "System components" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 for an illustrated view of the mechanical components.

NOTE

All parts illustrated in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 are not FRUs (Field replaceable Units). Refer to the AW Server 3.2 Installation and Service Manual, HPE ProLiant ML350p Gen8 Server Low Tier – Hardware FRU's for information about the mechanical parts that are stored as FRU at GEHC warehouses.

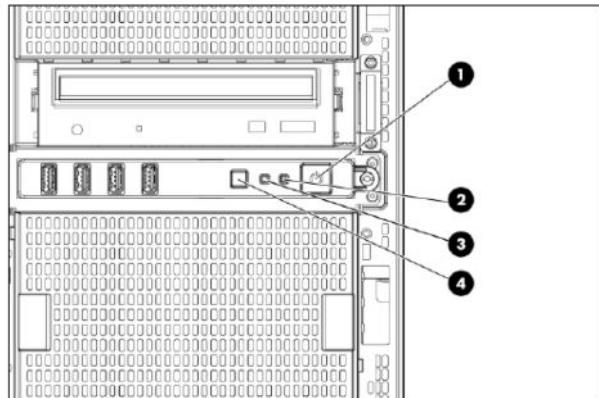
3.9.3 HPE ProLiant ML350p Gen8 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.9.3.1 HPE ProLiant ML350p Gen8 Server front panel LEDs codes

Refer to section "Front panel LEDs and buttons" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.



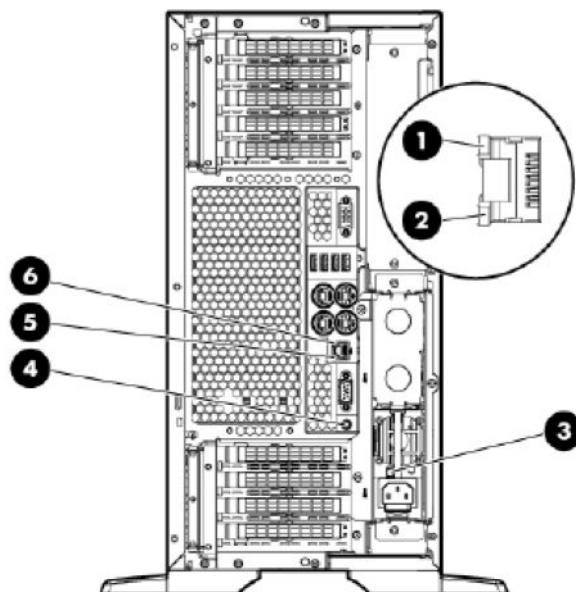
| Item | Description | Status |
|------|--|--|
| 1 | Power On/Standby button and system power LED | Solid green = System on
Flashing green (1 Hz/cycle per sec) = Performing power on sequence
Solid amber = System in standby
Off = No power present* |
| 2 | NIC status LED | Solid green = Link to network
Flashing green (1 Hz/cycle per sec) = Network active
Off = No network activity |
| 3 | Health LED | Solid green = Normal
Flashing amber = System degraded
Flashing red (1 Hz/cycle per sec) = System critical
Fast-flashing red (4 Hz/cycles per sec) = Power fault** |
| 4 | UID button/LED | Solid blue = Activated
Flashing blue (1 Hz/cycle per sec) = Remote management or firmware upgrade in progress
Off = Deactivated |

*Facility power is not present, power cord is not attached, no power supplies are installed, power supply failure has occurred, or the power button cable is disconnected.

**To identify components in a degraded or critical state, see the Systems Insight Display LEDs ("Systems Insight Display assembly" on page 53), check iLO/BIOS logs, and reference the server troubleshooting guide.

3.9.3.2 HPE ProLiant ML350p Gen8 Server rear panel LEDs codes

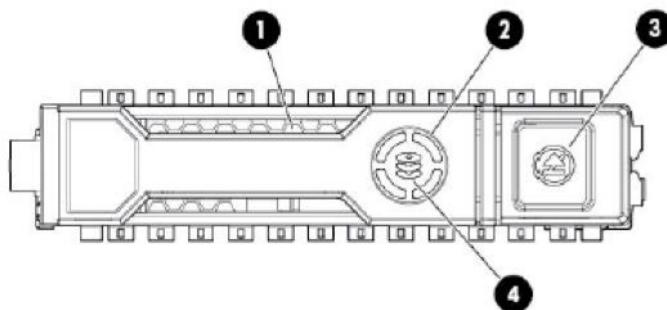
Refer to section "Rear panel LEDs" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.



| Item | Description | Status |
|------|--------------------|--|
| 1 | NIC activity LED | Green or flashing green = Network activity
Off = No network activity |
| 2 | NIC link LED | Green = Linked to network
Off = No network connection |
| 3 | Power supply LED | Green = Normal
Off = One or more of the following conditions exists: <ul style="list-style-type: none">• Power is unavailable.• Power supply failed.• Power supply is in standby mode.• Power supply exceeded current limit. |
| 4 | UID LED | Blue = Activated
Flashing blue = System is being managed remotely
Off = Deactivated |
| 5 | iLO 4 link LED | Green = Linked to network
Off = No network connection |
| 6 | iLO 4 activity LED | Green or flashing green = Network activity
Off = No network activity |

3.9.3.3 HPE ProLiant ML350p Gen8 Server SAS or SATA hard drive LED codes

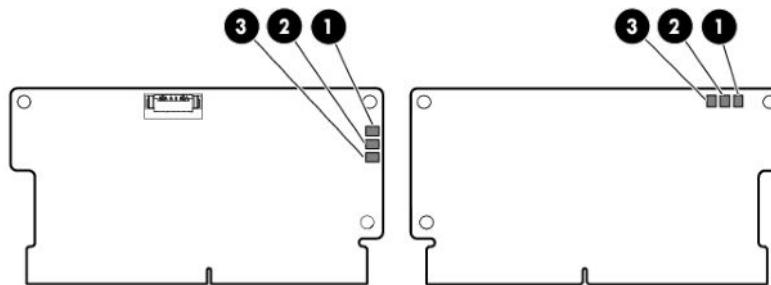
Refer to section "Hot-plug drive LED definitions" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.



| Item | LED | Status | Definition |
|------|---------------|----------------------|--|
| 1 | Locate | Solid blue | The drive is being identified by a host application. |
| | | Flashing blue | The drive carrier firmware is being updated or requires an update. |
| 2 | Activity ring | Rotating green | Drive activity |
| | | Off | No drive activity |
| 3 | Do not remove | Solid white | Do not remove the drive. Removing the drive causes one or more of the logical drives to fail. |
| | | Off | Removing the drive does not cause a logical drive to fail. |
| 4 | Drive status | Solid green | The drive is a member of one or more logical drives. |
| | | Flashing green | The drive is rebuilding or performing a RAID migration, strip size migration, capacity expansion, or logical drive extension, or is erasing. |
| | | Flashing amber/green | The drive is a member of one or more logical drives and predicts the drive will fail. |
| | | Flashing amber | The drive is not configured and predicts the drive will fail. |
| | | Solid amber | The drive has failed. |
| | | Off | The drive is not configured by a RAID controller. |

3.9.3.4 HPE ProLiant ML350p Gen8 Server FBWC module LEDs codes

The Flash Backed Write Cache (FBWC) module has three single-color LEDs (one amber and two green). The LEDs on the cache module installed on a storage controller are duplicated on the reverse side of the module to facilitate status viewing. Refer to section "FBWC module LEDs (P222, P420, P420i, P421, P822)" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.



| 1 - Amber | 2 - Green | 3 - Green | Interpretation |
|---------------|-----------------|-----------------|---|
| Off | Off | Off | The cache module is not powered. |
| Off | Flashing 0.5 Hz | Flashing 0.5 Hz | The cache microcontroller is executing from within its boot loader and receiving new flash code from the host controller. |
| Off | Flashing 1 Hz | Flashing 1 Hz | The cache module is powering up, and the capacitor pack is charging. |
| Off | Off | Flashing 1 Hz | The cache module is idle, and the capacitor pack is charging. |
| Off | Off | On | The cache module is idle, and the capacitor pack is charged. |
| Off | On | On | The cache module is idle, the capacitor pack is charged, and the cache contains data that has not yet been written to the drives. |
| Off | Flashing 1 Hz | Off | A backup is in progress. |
| Off | On | Off | The current backup is complete with no errors. |
| Flashing 1 Hz | Flashing 1 Hz | Off | The current backup failed, and data has been lost. |
| Flashing 1 Hz | Flashing 1 Hz | On | A power error occurred during the previous or current boot. Data might be corrupt. |
| Flashing 1 Hz | On | Off | An overtemperature condition exists. |
| Flashing 2 Hz | Flashing 2 Hz | Off | The capacitor pack is not attached. |
| Flashing 2 Hz | Flashing 2 Hz | On | The capacitor has been charging for 10 minutes, but has not reached sufficient charge to perform a full backup. |
| On | On | Off | The current backup is complete, but power fluctuations occurred during the backup. |
| On | On | On | The cache module microcontroller has failed. |

3.9.4 Troubleshooting HPE ProLiant ML350p Gen8 Server memory problems

1. Isolate and minimize the memory configuration. Use care when handling DIMMs.
Refer to section "Preventing electrostatic discharge" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.
2. Be sure the memory meets the server requirements and is installed as required by the server. Some servers may require that memory banks be populated fully or that all memory within a memory bank must be the same size, type, and speed. To determine if the memory is installed properly, see the server documentation.
3. Check any server LEDs that correspond to memory slot.

4. If you are unsure which DIMM has failed, test each bank of DIMMs by removing all other DIMMs. Then, isolate the failed DIMM by switching each DIMM in DIMM.
5. Remove any third-party memory.

3.9.5 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.9.6 HPE ProLiant ML350p Gen8 Server troubleshooting tips

| Problem | Solution |
|--|--|
| After one HDD was replaced and the system is rebooted, the IPMI driver hangs. Also the green led is blinking on the new HDD, while the leds for other HDD are steady green. | The root cause is that the Service Processor (iLO) and the main system lost connection.
The solution is to unplug all power cables, wait a few minutes, re-plug and start the system. |
| <ul style="list-style-type: none"> • The server does not power on. • The system power LED is off or amber. • The external health LED is red, flashing red, amber, or flashing amber. The internal health LED is red, flashing red, amber, or flashing amber. • The system health LED is red, flashing red, amber, or flashing amber. | <ul style="list-style-type: none"> • Improperly seated or faulty power supply • Loose or faulty power cord • Power source problem • Improperly seated component or interlock problem |

Following the HPE ProLiant ML350p Gen8 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

NOTE

Use either the `ssacli` command or the `hpssacli` command. The commands displayed below use `ssacli`. If `ssacli` is not available, replace it by `hpssacli`.

| Device | Instructions / Linux Command | Parameters |
|----------------------|--|---|
| Information | <code>sosreport</code>
<code>(/usr/sbin/sosreport)</code> | System hardware information |
| Internal controller | <code>/usr/sbin/ssacli controller slot=0 show</code> | Battery/capacitor status
Controller status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 logicaldrive all show</code> | Internal logical drive status |
| Internal disk status | <code>/usr/sbin/ssacli controller slot=0 physicaldrive all show</code> | Individual physical drive status |

| Device | Instructions / Linux Command | Parameters |
|--------------------------------|--|--|
| Internal server sea of sensors | <pre>ipmitool sensor egrep 'RPM degrees Volts Watts Fan'</pre> <p>NOTE</p> <ul style="list-style-type: none"> The PowerMeter info shall not be taken into account. The status of Power supplies and Fans is nc by default. The status of temperature sensors is na by default. | Power supplies status
Fans status
Temperature sensors status |

Example of result of disk status "physicaldrive"

Type the following command:

```
/usr/sbin/hpssacli controller slot=0 physicaldrive all show <Enter> OR
```

```
/usr/sbin/ssaci controller slot=0 physicaldrive all show <Enter>
```

Smart Array P410i in Slot 0 (Embedded)

array A (This is the system disks array)

physicaldrive 1I:1:1 (port 1I:box 1:bay 1, SATA, 500 GB, OK)

physicaldrive 1I:1:2 (port 1I:box 1:bay 2, SATA, 500 GB, OK)

array B (This is the image disks array)

physicaldrive 2I:1:5 (port 2I:box 1:bay 5, SATA, 500 GB, OK)

physicaldrive 2I:1:6 (port 2I:box 1:bay 6, SATA, 500 GB, OK)

physicaldrive 2I:1:7 (port 2I:box 1:bay 7, SATA, 500 GB, OK)

physicaldrive 2I:1:8 (port 2I:box 1:bay 8, SATA, 500 GB, Predictive Failure)

In our example, the 6th physical drive of the HPE ProLiant ML350p Gen8 Server is reporting some issues and predicts to fail in a close future. This drive has to be replaced as soon as possible.

Looking at the drive itself, you may also see an orange blinking LED reporting the predictive failure.

3.9.7 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the 70-persistent-net.rules file with the the following command:

```
/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>
```

3. Reboot the server.

```
reboot <Enter>
```

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:

- a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.10 HP ProLiant ML350 G6 Server hardware troubleshooting

For more details on this section, refer to the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009, and follow instructions of section "Component identification".

NOTICE

The HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 is a generic document and is given for information only. Not all sections apply to the AW Server product.

3.10.1 HP ProLiant ML350 G6 Server mechanical components description

Refer to section "Mechanical components" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009, for an illustrated view of the mechanical components.

NOTE

All parts illustrated in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 are not FRUs (Field replaceable Units). Refer to the AW Server 3.2 Installation and Service Manual, HP ProLiant ML350 G6 Server Low Tier – Hardware FRU's for information about the mechanical parts that are stored as FRU at GEHC warehouses.

3.10.2 HP ProLiant ML350 G6 Server system components description

Refer to section "System components" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 for an illustrated view of the system components.

NOTE

All parts illustrated in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 are not FRUs (Field replaceable Units). Refer to AW Server 3.2 Installation and Service Manual, HP ProLiant ML350 G6 Server Low Tier – Hardware FRU's for information about the system parts that are stored as FRU at GEHC warehouses.

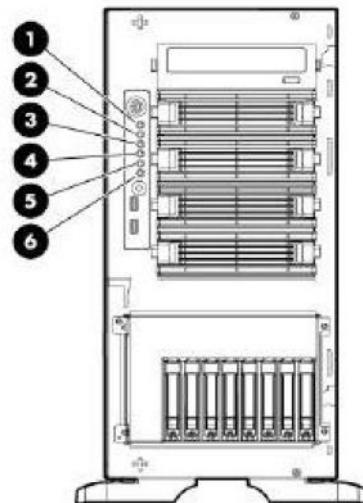
3.10.3 HP ProLiant ML350 G6 Server component identification and LED code meaning

The main serviceable items of the workstation are provided with LEDs, which light code helps identifying proper working condition of the server or an error condition.

Refer to sections below.

3.10.3.1 HP ProLiant ML350 G6 Server front panel LEDs code meaning

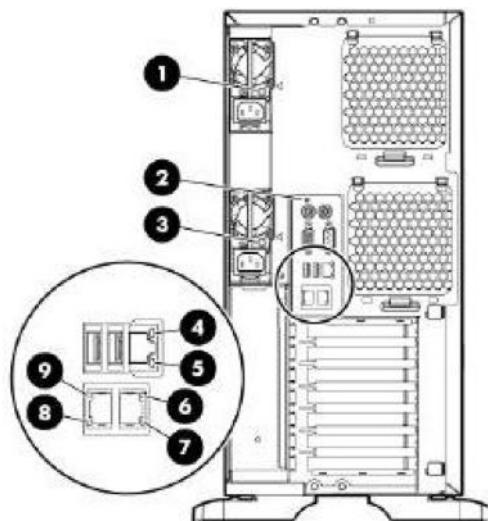
Refer to section "Front panel LEDs and buttons" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009.



| Item | Description | Status |
|------|--------------------|---|
| 1 | System power LED | Green = Power on
Flashing green = Waiting for power due to group power capping
Amber = System in standby, but power still applied
Off = Power cord not attached or power supply failure |
| 2 | Health LED | Green = Normal
Amber = System degraded. To identify the component in a degraded state, see the system board LEDs
Red = System critical. To identify the component in a critical state, see the system board LEDs
Off = Normal (when in standby mode) |
| 3 | Power cap LED | Green = Power cap configured
Flashing amber = Power cap exceeded
Off = Server in standby or power cap disabled |
| 4 | NIC 1 activity LED | Green = Network link
Flashing = Network link and activity
Off = No link to network. If power is off, view status on the rear panel RJ-45 LEDs |
| 5 | NIC 2 activity LED | Green = Network link
Flashing = Network link and activity
Off = No link to network. If power is off, view status on the rear panel RJ-45 LEDs |
| 6 | UID LED | Blue = Activated
Flashing = System managed remotely
Off = Deactivated |

3.10.3.2 HP ProLiant ML350 G6 Server rear panel LEDs code meaning

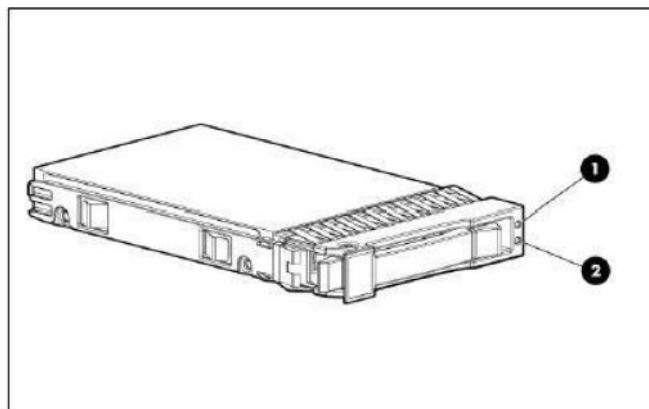
Refer to section "Component identification" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009.



| Item | Description | Status |
|------|--------------------|---|
| 1 | Power supply 2 LED | Green = Power supply is on and functioning.
Off = AC power is not available or AC power supply has failed. |
| 2 | UID LED | Blue = Activated
Flashing blue = System managed remotely
Off = Deactivated |
| 3 | Power supply 1 LED | Green = Power supply is on and functioning.
Off = AC power is not available or AC power supply has failed. |
| 4 | iLO 2 link LED | Green = Linked to network
Off = Not linked to network |
| 5 | iLO 2 activity LED | Green or flashing = Network activity
Off = No network activity |
| 6 | NIC 2 link LED | Green = Linked to network
Off = Not linked to network |
| 7 | NIC 2 activity LED | Green or flashing = Network activity
Off = No network activity |
| 8 | NIC 1 link LED | Green = Linked to network
Off = Not linked to network |
| 9 | NIC 1 activity LED | Green or flashing = Network activity
Off = No network activity |

3.10.3.3 HP ProLiant ML350 G6 Server SAS or SATA hard drive LED combinations

Refer to sections "SAS and SATA drive LEDs" and "SAS and SATA hard drive LED combinations" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009.



Fault/UID LED (amber/blue)

Online LED (green)

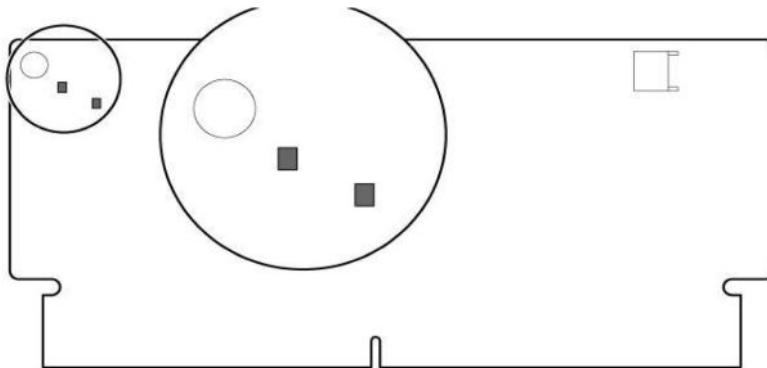
| Online/activity LED (green) | Fault/UID LED (amber/blue) | Interpretation |
|-----------------------------|----------------------------------|--|
| On, off, or flashing | Alternating amber and blue | The drive has failed, or a predictive failure alert has been received for this drive; it also has been selected by a management application. |
| On, off, or flashing | Steadily blue | The drive is operating normally, and it has been selected by a management application. |
| On | Amber, flashing regularly (1 Hz) | A predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| On | Off | The drive is online, but it is not active currently. |
| Flashing regularly (1 Hz) | Amber, flashing regularly (1 Hz) | Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.
The drive is part of an array that is undergoing capacity expansion or stripe migration, but a predictive failure alert has been received for this drive. To minimize the risk of data loss, do not replace the drive until the expansion or migration is complete. |
| Flashing regularly (1 Hz) | Off | Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.
The drive is rebuilding, erasing, or it is part of an array that is undergoing capacity expansion or stripe migration. |
| Flashing irregularly | Amber, flashing regularly (1 Hz) | The drive is active, but a predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| Flashing irregularly | Off | The drive is active, and it is operating normally. |
| Off | Steadily amber | A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible. |
| Off | Amber, flashing regularly (1 Hz) | A predictive failure alert has been received for this drive. Replace the drive as soon as possible. |
| Off | Off | The drive is offline, a spare, or not configured as part of an array. |

3.10.3.4 HP ProLiant ML350 G6 Server FBWC for RAID (Flash Backed Write Cache) module LEDs code meaning

The Flash Backed Write Cache (FBWC) feature has two modules:

- The FBWC Cache module
- The FBWC capacitor pack

The FBWC Cache module has two single-color LEDs (green and amber). The LEDs are duplicated on the reverse side of the cache module to facilitate status viewing.



Green LED and Amber LED Interpretation

| Green LED | Amber LED | Interpretation |
|----------------|-----------|---|
| Off | On | A backup is in progress. |
| Flashing (1Hz) | On | A restore is in progress. |
| Flashing (1Hz) | Off | The capacitor pack is charging. |
| On | Off | The capacitor pack has completed charging |

The capacitor pack may need to be replaced for LED status below:

| Green LED | Amber LED | Interpretation |
|---|---|--|
| Flashing (2Hz) . Alternating with amber LED | Flashing (2Hz) . Alternating with green LED | One of the following conditions exists: <ul style="list-style-type: none"> The charging process has timed out The capacitor pack is not connected. |

The Cache module is to be replaced for LED status below:

| Green LED | Amber LED | Interpretation |
|-----------|-----------|-------------------------------------|
| On | On | The flash code image failed to load |
| On | Off | The flash code is corrupt |

Refer to section "FBWC module LEDs" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009.

3.10.4 Troubleshooting HP ProLiant ML350 G6 Server memory problems

1. Isolate and minimize the memory configuration. Use care when handling DIMMs.
Refer to section "Preventing electrostatic discharge" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009.
2. Be sure the memory meets the server requirements and is installed as required by the server. Some servers may require that memory banks be populated fully or that all memory within a memory bank must be the same size, type, and speed. To determine if the memory is installed properly, see the server documentation.
3. Check any server LEDs that correspond to memory slot.
4. If you are unsure which DIMM has failed, test each bank of DIMMs by removing all other DIMMs. Then, isolate the failed DIMM by switching each DIMM in DIMM.
5. Remove any third-party memory.

3.10.5 HPE Insight Diagnostics

NOTICE

The HPE Insight Diagnostics utility from HPE is not supported with the AW Server.

For information only:

HPE Insight Diagnostics is a proactive server management tool, available in both offline and online versions, that provides diagnostics, troubleshoots problems, and performs repair validation. HPE Insight Diagnostics Offline Edition performs various in-depth system and component testing while the OS is not running. To run this utility, launch the SmartStart CD. HPE Insight Diagnostics Online Edition is a web-based application that captures system configuration and other related data needed for effective server management. Available in Microsoft® Windows® and Linux versions, the utility helps to ensure proper system operation.

3.10.6 HP ProLiant ML350 G6 Server troubleshooting tips

| Problem | Solution |
|--|--|
| After one HDD was replaced and the system is rebooted, the IPMI driver hangs. Also the green led is blinking on the new HDD, while the leds for other HDD are steady green. | The root cause is that the Service Processor (iLO) and the main system lost connection.
The solution is to unplug all power cables, wait a few minutes, re-plug and start the system. |
| <ul style="list-style-type: none"> • The server does not power on. • The system power LED is off or amber. • The external health LED is red, flashing red, amber, or flashing amber. The internal health LED is red, flashing red, amber, or flashing amber. • The system health LED is red, flashing red, amber, or flashing amber. | <ul style="list-style-type: none"> • Improperly seated or faulty power supply • Loose or faulty power cord • Power source problem • Improperly seated component or interlock problem |

Following the HP ProLiant ML350 G6 Server hardware issue detected (disk, fan, power supply, controller), run the appropriate command among the following:

NOTE

Use either the **hpacucli** command or the **hpssacli** command, when available for the HPE server types. The commands displayed below use **hpssacli**. If this command is not available, replace it by the **hpacucli**.

| Device | Instructions / Linux Command | Parameters |
|----------------------|--|---|
| Information | sosreport
(/usr/sbin/sosreport) | System hardware information |
| Internal controller | /usr/sbin/hpssacli controller slot=0 show | Battery/capacitor status
Controller status |
| Internal disk status | /usr/sbin/hpssacli controller slot=0 logicaldrive all show | Internal logical drive status |
| Internal disk status | /usr/sbin/hpssacli controller slot=0 physicaldrive all show | Individual physical drive status |

| Device | Instructions / Linux Command | Parameters |
|--------------------------------|--|--|
| Internal server sea of sensors | <pre>ipmitool sensor egrep 'RPM degrees Volts Watts Fan'</pre> <p>NOTE</p> <ul style="list-style-type: none"> The PowerMeter info shall not be taken into account. The status of Power supplies and Fans is nc by default. The status of temperature sensors is na by default. | Power supplies status
Fans status
Temperature sensors status |

Example of result of disk status "physicaldrive":

Type the following command:

```
/usr/sbin/hpacucli controller slot=0 physicaldrive all show<Enter> OR
/usr/sbin/hpssacli controller slot=0 physicaldrive all show<Enter>
Smart Array P410i in Slot 0 (Embedded)
array A (This is the system disks array)
physicaldrive 1I:1:1 (port 1I:box 1:bay 1, SATA, 500 GB, OK)
physicaldrive 1I:1:2 (port 1I:box 1:bay 2, SATA, 500 GB, OK)
array B (This is the image disks array)
physicaldrive 1I:1:3 (port 1I:box 1:bay 3, SATA, 500 GB, OK)
physicaldrive 1I:1:4 (port 1I:box 1:bay 4, SATA, 500 GB, OK)
physicaldrive 2I:1:5 (port 2I:box 1:bay 5, SATA, 500 GB, OK)
physicaldrive 2I:1:6 (port 2I:box 1:bay 6, SATA, 500 GB, Predictive Failure)
```

In our example, the 6th physical drive of the HP ProLiant ML350 G6 Server is reporting some issues and predicts to fail in a close future. This drive will have to be replaced as soon as possible.

Looking at the drive itself, you may also see an orange blinking LED reporting the predictive failure.

3.10.7 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the 70-persistent-net.rules file with the the following command:

```
/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>
```
3. Reboot the server.

```
reboot <Enter>
```

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

3.11 HP RAID / Disk Subsystem

3.11.1 DAS (Direct Attached Storage) for HPE ProLiant DL580 G7 Server / HPE ProLiant DL560 Gen8 Server High Tier

The High Tier Hardware is connected to a DAS (Direct Attached Storage). Note that the Low Tier server as well as the HPE ProLiant DL360 Gen10 Server / HPE ProLiant DL360 Gen9 Server has no separate DAS as the storage is internal to the server.

The older HP D2600 DAS is end of production and has been replaced by a similar DAS, the HP D3600 DAS. There is no main difference between the new and older DAS.

The HP D2600 DAS / HP D3600 DAS is fitted with 12 × HP 1TB SATA 7.2K rpm LFF (3.5-inch) hard disk drives, and has two power supplies for redundancy.

It also has two I/O modules, only one being used to connect to the HPE ProLiant DL560 Gen8 Server, same as for HP D2600 DAS.



HP DAS D2600



HP DAS D3600 without protection grid



HP DAS D3600 with protection grid

NOTE

The HP D3600 DAS is delivered with a long (2 meters) data cable. DO NOT order part number 5610644 (long data cable) that is dedicated to the HP D2600 DAS and cannot be used (different connectors).

NOTE

The metallic label, to be stuck on top of the DAS is no longer delivered, as becoming useless

3.11.2 RAID / Disk Subsystem Setup Information

The initial hardware setup and configuration — including the internal and external storage disk drives — is the responsibility of the Vendor. Likewise, when there is a disk drive failure scenario, the Vendor will be responsible for replacing and re-configuring the devices back to normal.

So, there is no in-depth configuration or trouble-shooting write-up regarding the disk / RAID setup for the AW Server system. However, here are a few high-level information points that need to be understood about the disk / RAID environment:

- The **SYSTEM** logical partition consists of **two** 3.5" SAS/SATA drives running in a **RAID 1** configuration:
 - 2 × 300GB for HPE ProLiant DL360 Gen10 Server and HPE ProLiant DL360 Gen9 Server (Low Tier and High Tier)
 - 2 × 500GB for HP ProLiant ML350 G6 Server and HPE ProLiant ML350p Gen8 Server
 - 2 × 1TB for HPE ProLiant ML350p Gen8 Server starting Q1 2017
 - 2 × 146GB for HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server
 - 2 × 300GB for HPE ProLiant DL560 Gen8 Server starting Q1 2017
 - There should be a **root** and **swap** partition on this virtual drive.
- The **IMAGE** logical partition consists of 3.5" SAS/SATA drives running in a **RAID 1+0** configuration:
 - 6 × 600GB HDD for HPE ProLiant DL360 Gen10 Server Low Tier
 - 4 × 500GB for HP ProLiant ML350 G6 Server and HPE ProLiant ML350p Gen8 Server
 - 4 × 1TB for HPE ProLiant ML350p Gen8 Server starting Q1 2017
 - 12 × 1TB for HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server.
- The **IMAGE** logical partition consists of SAS drives running in a **RAID 6** configuration:
 - 6 × 1.8TB HDD for HPE ProLiant DL360 Gen10 Server High Tier
 - 4 × 600GB HDD for HPE ProLiant DL360 Gen9 Server Low Tier
 - 4 × 1.8TB HDD for HPE ProLiant DL360 Gen9 Server High Tier

SAS - Serial Attached SCSI drive - is a data transfer technology designed to move data to and from computer storage devices such as hard drives. It is a point-to-point serial protocol that replaces the parallel SCSI bus technology, and uses the standard SCSI command set.

SATA - Serial Advanced Technology Attachment drive - is a computer bus primarily designed for transfer of data between a computer and mass storage devices such as hard disk drives. The main advantages are faster data transfer, ability to remove or add devices while operating (**hot swapping**), thinner cables that let air cooling work more efficiently, and more reliable operation with tighter data integrity checks.

SSD - Solid-State Drive (also known as a solid-state disk) is a solid-state storage device that uses integrated circuit assemblies as memory to store data persistently. SSD technology primarily uses electronic interfaces compatible with traditional block input/output (I/O) hard disk drives (HDDs).

RAID 1 - Redundant Array of Inexpensive Disks - Mirrored set without parity — This configuration provides fault tolerance from disk errors and failure of all but one of the drives. Array continues to operate so long as at least one drive is functioning.

RAID 1+0 (RAID10) - Redundant Array of Inexpensive Disks - RAID10 is one of the combinations of RAID 1 (mirroring) and RAID 0 (striping) which are possible. RAID 10 stripes data across half of the disk drives in the RAID 10 configuration. The other half of the array mirrors the first set of disk drives. Access to data is preserved if one disk in each mirrored pair remains available. RAID 10 can offer

faster data reads and writes than RAID 5 because it does not need to manage parity. However, with half of the drives in the group used for data and the other half used to mirror that data, RAID 10 disk groups have less capacity than RAID 5 disk groups.

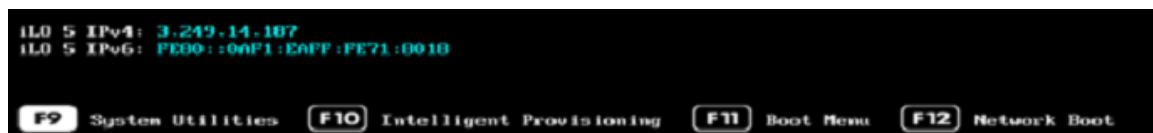
RAID 6 - Redundant Array of Inexpensive Disks - RAID 6, also known as double-parity RAID, uses two parity stripes on each disk. It allows for two disk failures within the RAID set before any data is lost. RAID 6 extends RAID 5 by adding another parity block; thus, it uses block-level striping with two parity blocks distributed across all member disks.

3.11.3 Configuring the HPE ProLiant DL360 Gen10 Server RAID

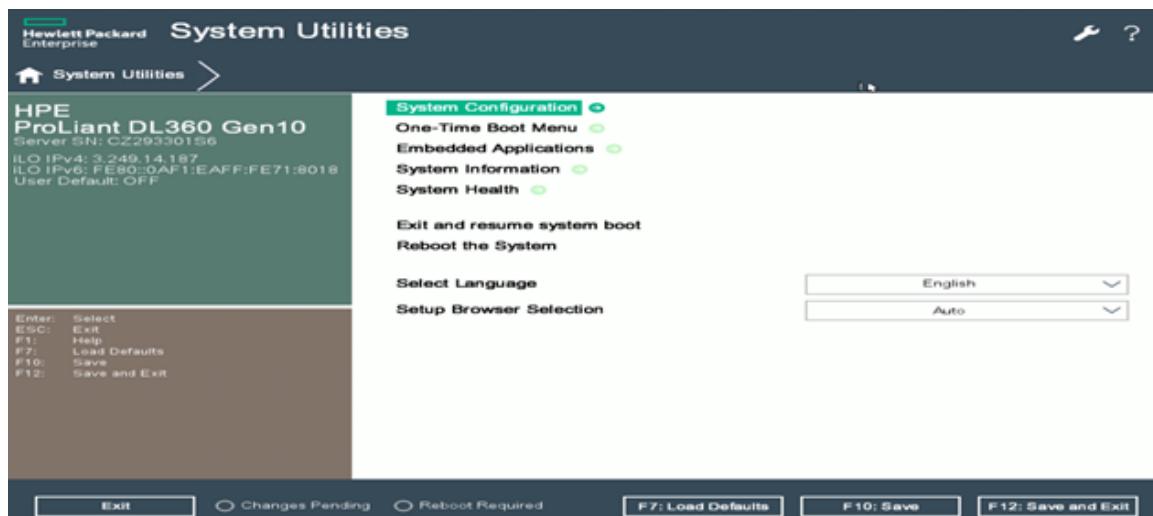
NOTE

The following is applicable to the HPE ProLiant DL360 Gen10 Server. For the HPE ProLiant DL360 Gen9 Server, refer to [3.11.4 Configuring the HPE ProLiant DL360 Gen9 Server RAID on page 335](#). For the HP ProLiant ML350 G6 Server, HPE ProLiant ML350p Gen8 Server, HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server, refer to [3.11.5 Configuring the RAID on page 339](#).

- During a system boot, press **<F9>** to open the BIOS System Utilities.

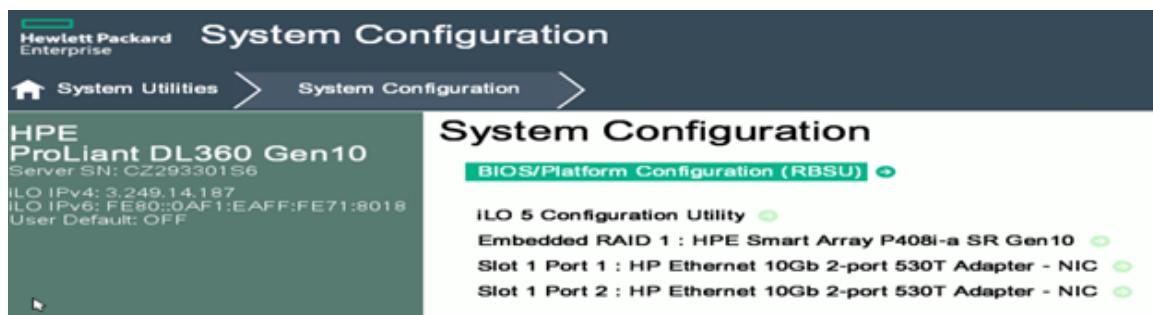


The *System Utilities* menu opens.



- Click on **System Configuration**.

The *System Configuration* menu opens.



3. In *System Configuration*, click on the **Embedded RAID 1 : HPE Smart Array...** link to activate the *HPE Smart Array* menu.
4. In the *HPE Smart Array* menu, click on the **Exit and launch HP Smart Storage Administrator (SSA)** link to activate the *Smart Storage Administrator* utility.

The *Smart Storage Administrator* utility initializes.

Several screens are displayed for a few moments then it enters into the *Welcome to Smart Storage Administrator* menu:



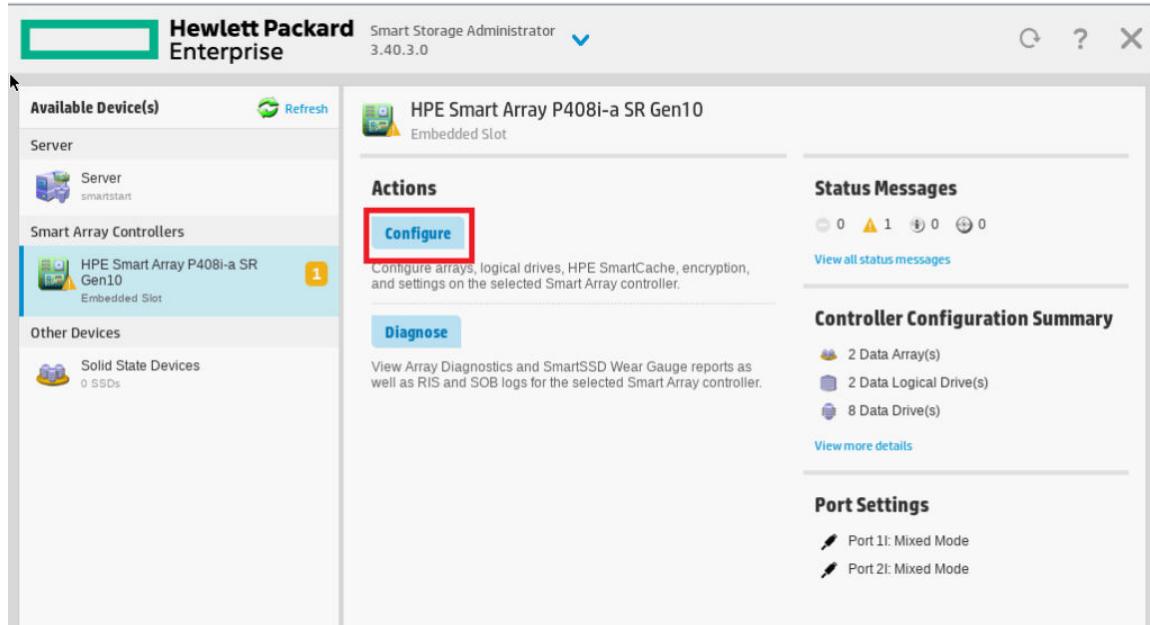
5. Click on the **HPE Smart Array ...** icon on the left side of the screen.

The **HPE Smart Array** menu displays.

NOTE

Once you have selected an *Actions* menu, to move back and forth between the **Diagnose** and **Configure** menus, click on the arrow on the top of screen then select the desired menu.

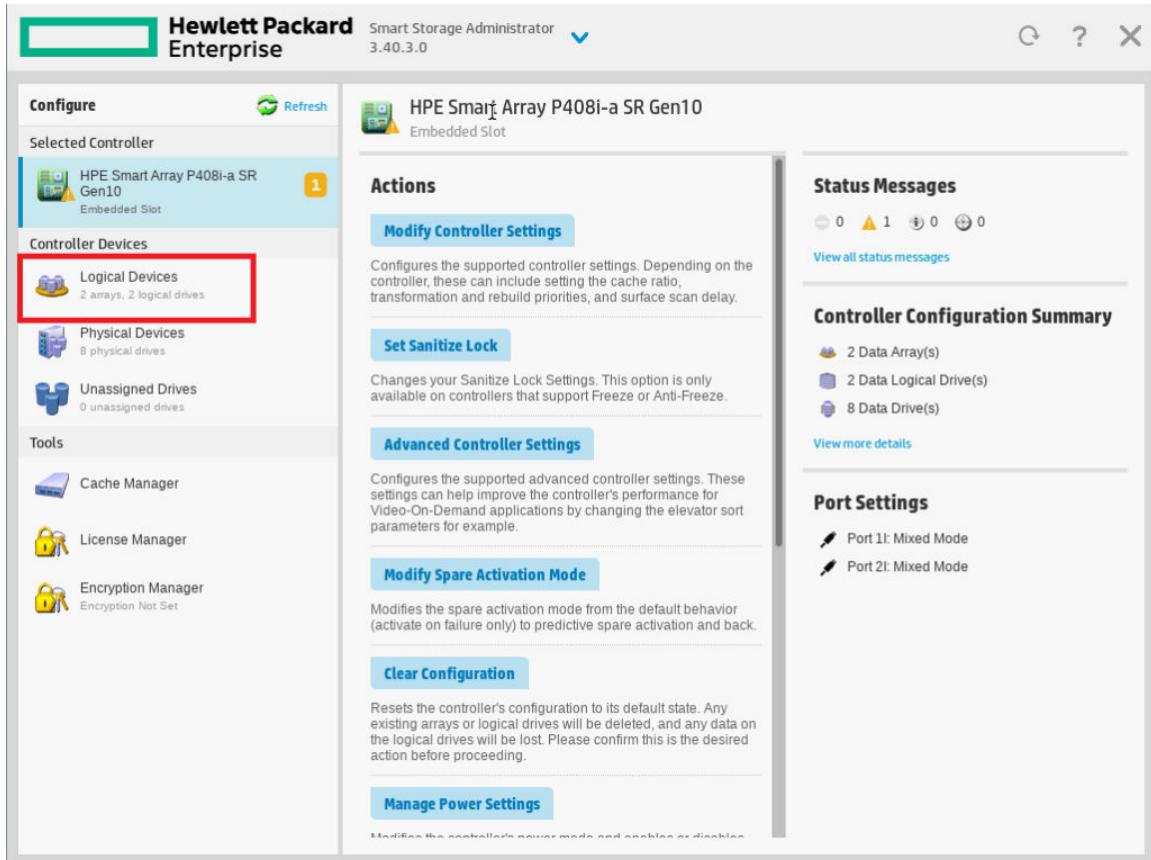
6. Click on the **Configure** button.



The *Configuration* menu opens.

7. Make sure that the following items are listed on the left part of the screen, under *Controller Devices*:
 - 2 logical drives
 - 8 physical drives
 - 0 unassigned drives

8. Click on the **Logical Devices** button.



The *Logical Devices* menu opens.

NOTE

The screenshot below is given as example. The actual disks configuration is made of Hard disk drives. Any future configuration may be made of SSD (solid state disks).

9. Make sure that **All** is selected from the **Show** drop down button.

The screenshot shows the 'Logical Devices' section of the Smart Storage Administrator interface. The 'Show' dropdown is set to 'All'. Two logical drives are highlighted with red boxes: 'Logical Devices' (under Controller Devices) and 'Array B - 1 Logical Drive(s)' (under Array Details). The 'Actions' panel includes a 'Delete Array' button.

| Logical Devices | |
|--------------------------------|----------------------------------|
| Logical A - 1 Logical Drive(s) | 0 MB (0.00%) Free Space |
| Logical Drive 1 | 279.37 GiB (299.97 GB), RAID 1 |
| 300 GB SAS HDD | Port 2i : Box 1 : Bay 7 |
| 300 GB SAS HDD | Port 2i : Box 1 : Bay 8 |
| Logical B - 1 Logical Drive(s) | 4 MB (0.00%) Free Space |
| Logical Drive 2 | 2.18 TiB (2.40 TB), RAID 6 (ADG) |
| 600 GB SAS HDD | Port 1i : Box 1 : Bay 1 |
| 600 GB SAS HDD | Port 1i : Box 1 : Bay 2 |
| 600 GB SAS HDD | Port 1i : Box 1 : Bay 3 |
| 600 GB SAS HDD | Port 1i : Box 1 : Bay 4 |
| 600 GB SAS HDD | Port 2i : Box 1 : Bay 5 |
| 600 GB SAS HDD | Port 2i : Box 1 : Bay 6 |

10. For HPE ProLiant DL360 Gen10 Server Low Tier, make sure that:

- Logical Drive 1 is setup as RAID 1 and has two 300 GB drives.
- Logical Drive 2 is setup as RAID 6 and has six 600 GB drives.

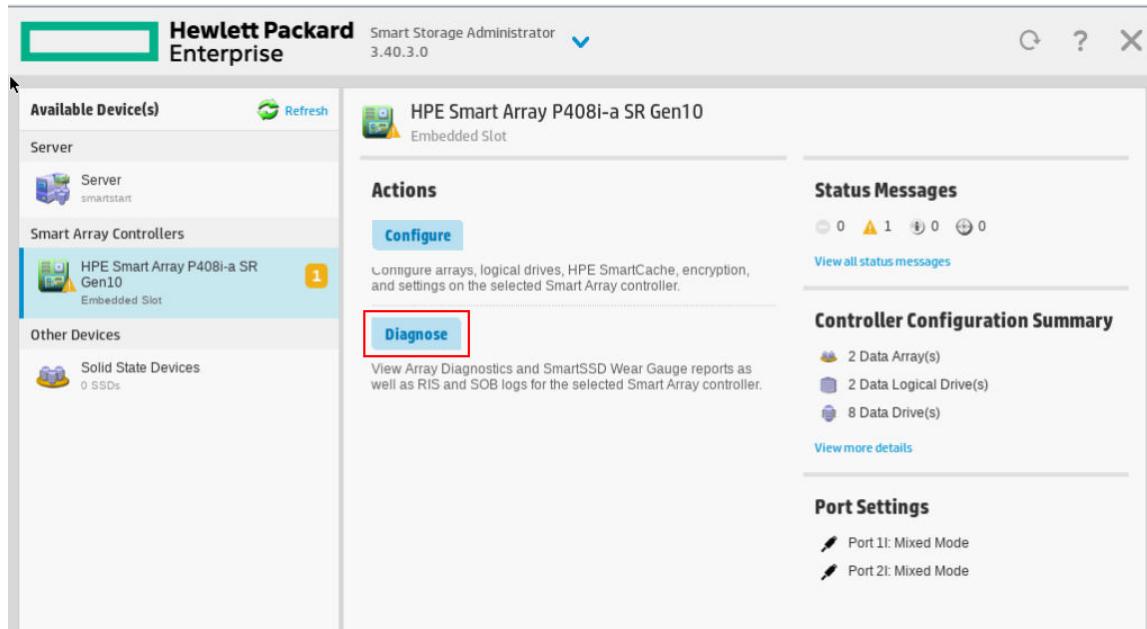
11. For HPE ProLiant DL360 Gen10 Server High Tier, make sure that:

- Logical Drive 1 is setup as RAID 1 and has two 300 GB drives.
- Logical Drive 2 is setup as RAID 6 and has six 1.8 TB drives.

NOTICE

If needed to modify the RAID settings, proceed with the section Re-creating logical drives on the HPE ProLiant DL360 Gen10 Server before exiting the *Smart Storage Administrator* tool.

12. To view Array diagnostics and reports, click on the **Diagnose** button.



3.11.4 Configuring the HPE ProLiant DL360 Gen9 Server RAID

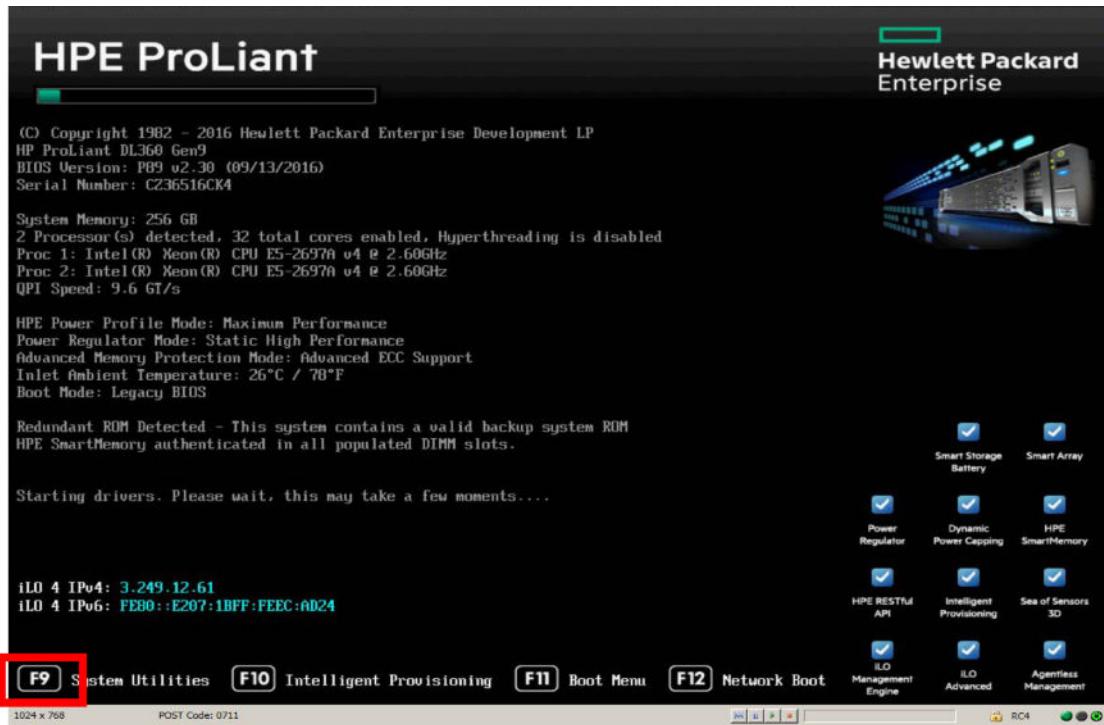
NOTE

The following is applicable to the HPE ProLiant DL360 Gen9 Server. For the HPE ProLiant DL360 Gen10 Server, refer to [3.11.3 Configuring the HPE ProLiant DL360 Gen10 Server RAID on page 331](#). For HP ProLiant ML350 G6 Server, HPE ProLiant ML350p Gen8 Server, HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server, refer to [3.11.5 Configuring the RAID on page 339](#).

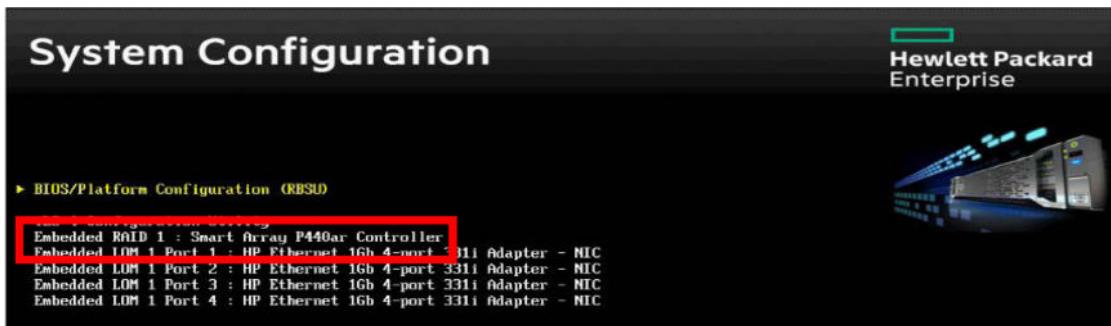
The configuration can start from the **System Utilities** or through **Intelligent Provisioning > Smart Storage Administrator**. The following describes the steps through the **System Utilities**.

1. Reboot the system.

2. Press **<F9>** to enter *System Utilities* when prompted.



3. Make sure **System Configuration** is selected and press **<Enter>**
- The BIOS setup menu displays after a moment.
4. Scroll down to **Embedded RAID 1: Smart Array P440ar Controller** and press **<Enter>**.



The *Smart Array P440ar Controller* setup menu opens.



5. Scroll down to **Exit and launch HP Smart Storage Administrator (HPSSA)** and press **<Enter>**.

The *Smart Storage Administrator* menu initializes. Several screens appear for a few moments then, the *Welcome to Smart Storage Administrator Menu* appears.

- Click on the **Smart Array P440ar** icon on the left side of the screen.



The **Smart Array P440ar** menu appears.

- To check the RAID status, click on the **View all status messages** link. To get more information on the System and Image arrays, click on the **View more details** link.



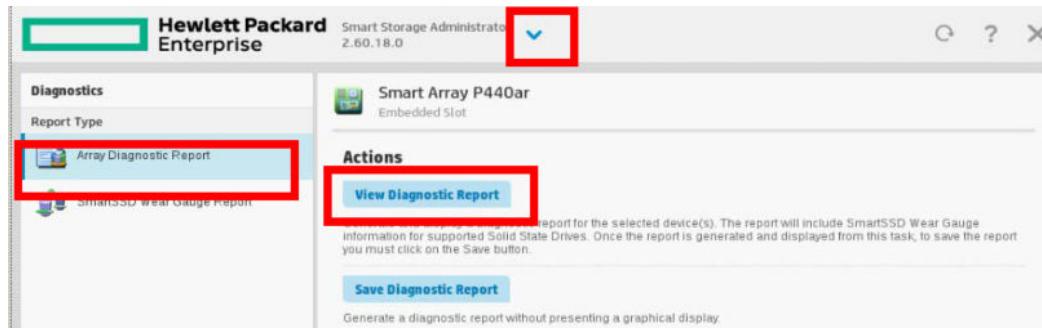
- Click on the **Close** button when done.
- To check or change the configuration of any of the arrays, click on the **Configure** button. To view Array diagnostics and reports, click on the **Diagnose** button.



NOTE

Once you have selected an Actions menu, to move back and forth between the **Diagnose** and **Configure** menus, click on the arrow on top of the screen then select the desired menu.

10. After clicking on the **Diagnose** button, select a diagnostic report then click on **View Diagnostic Report**.



NOTE

The screen shots below are given as example. The actual disks configuration is made of Hard disk drives. Any future configuration may be made of SSD (solid state) disks.

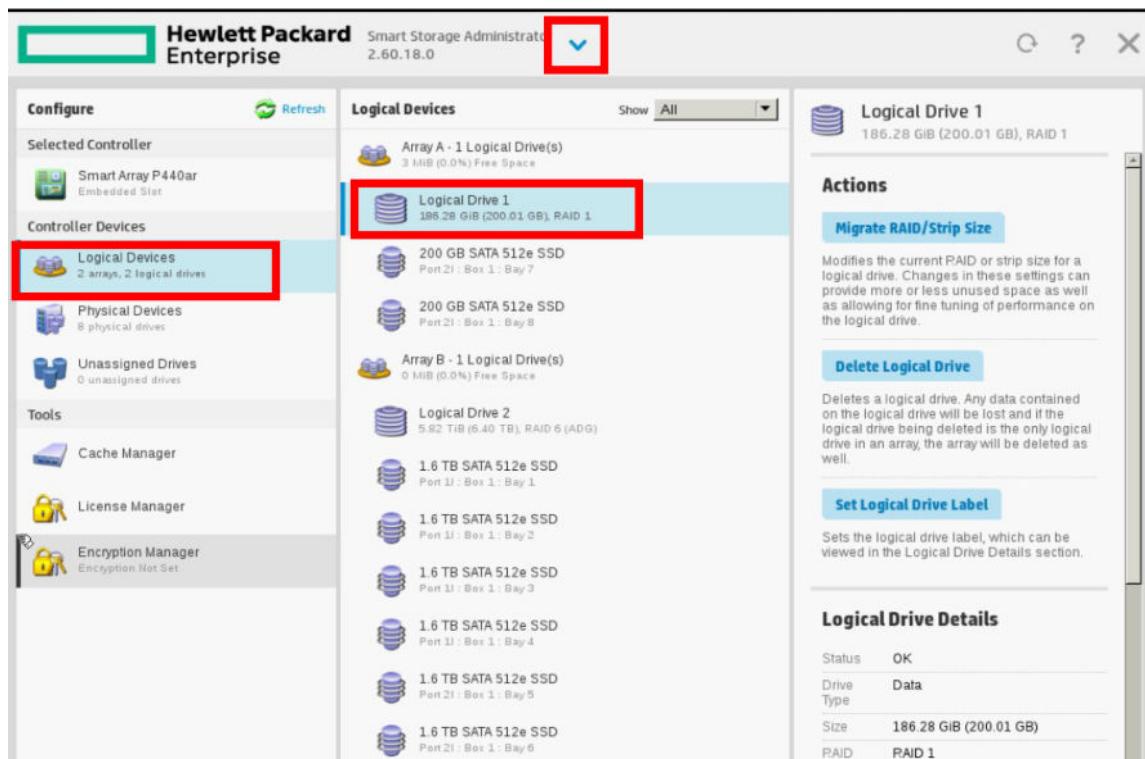
11. To return to the main menu, click on the **Close** button (of a report), then click on the arrow on top of the screen.
12. If you need to check or change the configuration of any of the arrays, click on the **Configure** button.

NOTICE

Changing any of the System or Image arrays parameters may in most cases lead to data loss and to the need of proceeding to complete software reload.

13. Check Controller devices:

- Check that you can see 2 arrays of 2 logical drives under the *Logical Devices* tab.
- Check that you can see 8 physical drives under the *Physical Devices* tab.
- Check that there are 0 (zero) unassigned drive.



14. Click on **Logical Devices** on the left part of the screen, then select **Logical Drive 1**.

15. Check that you can see a RAID1 logical drive of around 300GB composed of the two 300GB SAS HDDs.

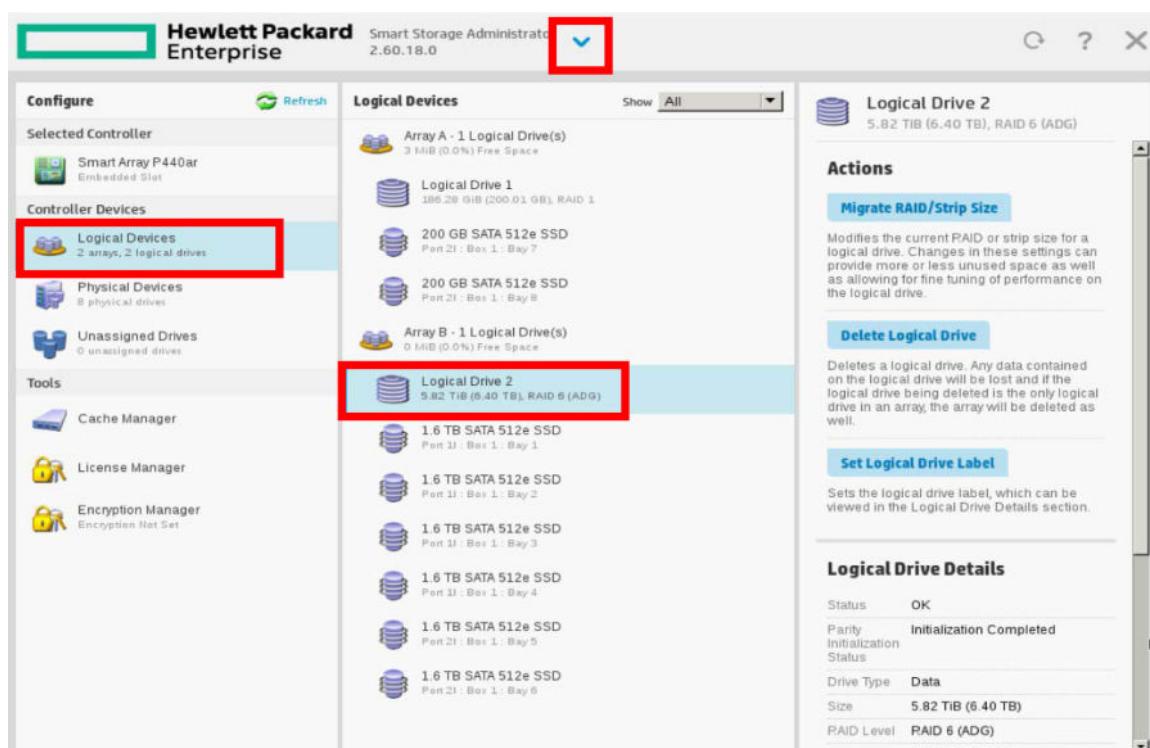
If it is not the case, you have to delete the logical drive and recreate a new one with the appropriate characteristics.

16. To delete the logical drive, click on the **Delete Logical Drive** button located on the right side of the screen and acknowledge the confirmation message.

NOTICE

Deleting the logical drive, all data will be lost, so software reload will be necessary.

17. When the logical drive is deleted, the **Delete Logical Drive** button changes to **Create Logical Drive**. Select the physical drives that should compose the logical drive and the proper RAID level.
18. When done with the first logical drive, select **Logical Drive 2**.



19. Check that you can see a RAID6 logical drive of around 6.4TB (High Tier) composed of the six 1.8TB SAS HDDs or a logical drive of around 1.6TB (Low Tier) composed of the six 600MB SAS HDDs
20. If it is not the case, delete the logical drive and re-create a new one with the appropriate characteristics as described before ([Step 16](#) to [Step 17](#)).

3.11.5 Configuring the RAID

NOTE

The following is applicable to the HP ProLiant ML350 G6 Server, HPE ProLiant ML350p Gen8 Server, HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server. For the HPE ProLiant DL360 Gen10 Server, refer to [3.11.3 Configuring the HPE ProLiant DL360 Gen10 Server RAID on page 331](#). For HPE ProLiant DL360 Gen9 Server, refer to [3.11.4 Configuring the HPE ProLiant DL360 Gen9 Server RAID on page 335](#).

NOTE

For more details on RAID configuration, refer to the AW Server 3.2 Hardware Installation Manual.

NOTE

The process described below is the process for the HP ProLiant ML350 G6 Server Low Tier. It is similar for other hardware like HPE ProLiant ML350p Gen8 Server Low Tier or HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server High Tier, but remember that the HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server have two controllers (1 controller for the internal 2 System hard disks and 1 controller for the 12 Image disks of the DAS).

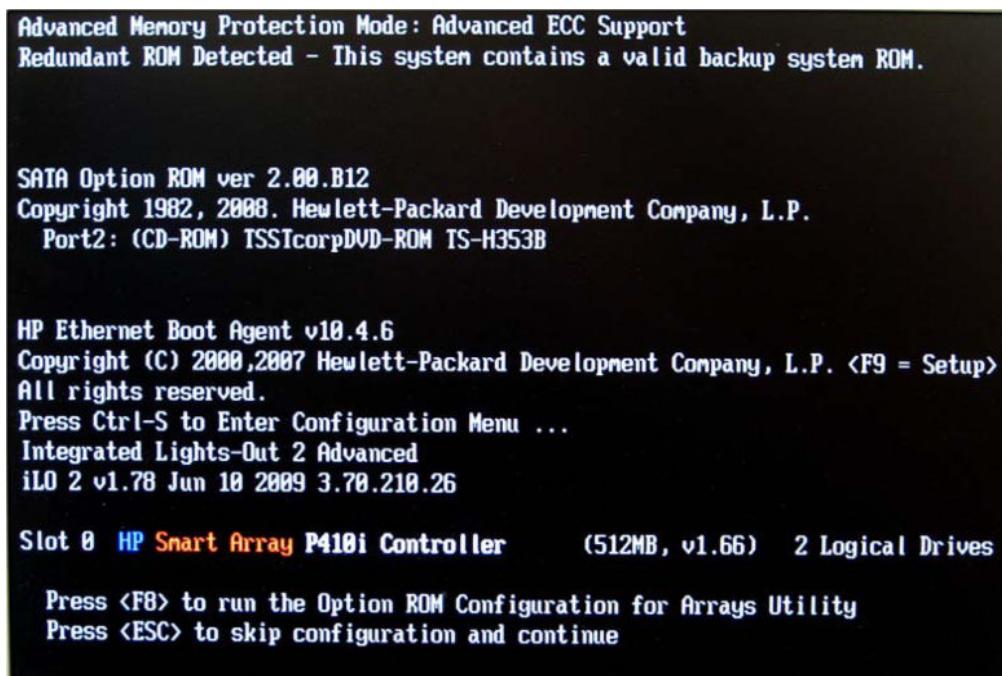
1. Reboot the system:

a. In a Terminal tool, login as **root <Enter>**.

b. Type:

reboot <Enter>

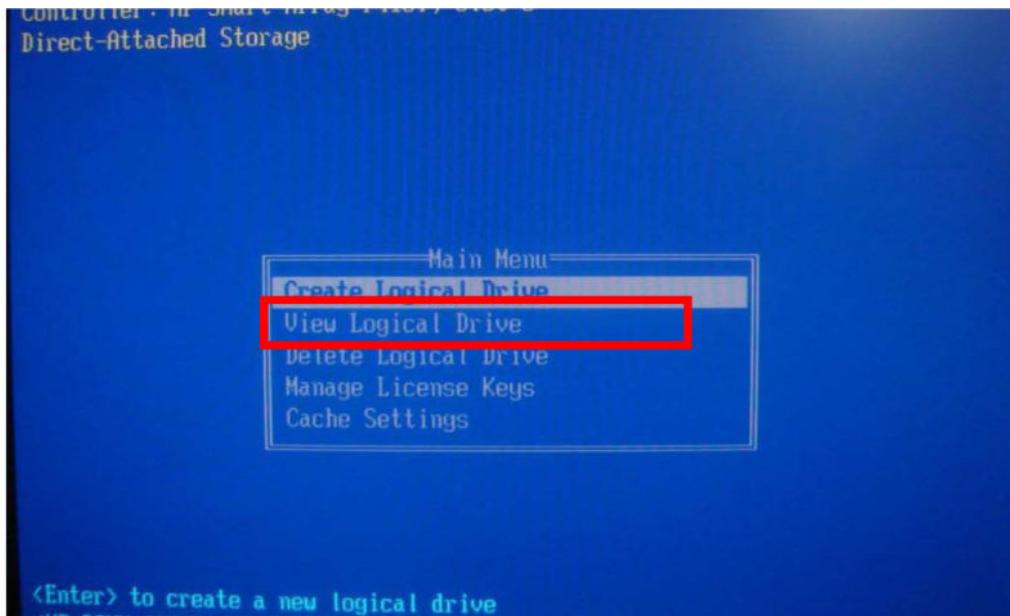
2. During the HP SmartArray P410i initialization process (example for the HP ProLiant ML350 G6 Server), enter the *Option Rom Configuration for Arrays* by pressing **<F8>**.

**NOTE**

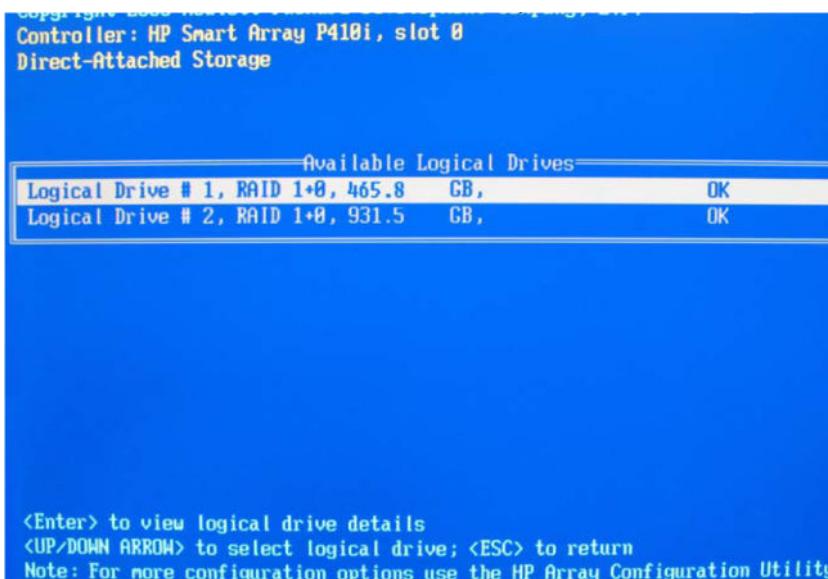
For the HPE ProLiant DL580 G7 Server and HPE ProLiant DL560 Gen8 Server, you will have to press **<F8>** a second time to enter the external image disks array (DAS) P411 / P421 controller setup, once done with the 2 internal System HDD controller. This step is not applicable for High Tier servers without DAS (in seamless integration).

3. The RAID logical drive configuration has been set up by the Vendor or GE Manufacturing, prior to delivering the HP ProLiant ML350 G6 Server / HPE ProLiant ML350p Gen8 Server server hardware to GEHC. To check RAID configuration, arrow down to **View Logical Drive**.

4. To modify the RAID setup when necessary, select **Delete Logical Drive** then select **Create Logical Drive**.



5. Verify that two logical drives have been configured, one in **RAID 1+0** with **465.8 GB** (500GB unformatted) and the other in **RAID 1+0** with **931.5 GB** (1TB unformatted).



6. Exit the *Option Rom Configuration for Arrays* by pressing **<Esc>**.

3.11.6 Various Configuration Checks

Once the OS has completed the boot up, login as **root**.

- To verify that the OS sees that the correct controllers are installed (see example for the ML350 G6) type the following command, and check results:

```
lspci | grep -i RAID <Enter>
```

```
04:00.0 RAID bus controller: Hewlett-Packard Company Smart Array G6
controllers (rev 01)
```

- To verify that OS has loaded the correct controller modules with the following command, and results

```
lsmod | grep -i aac <Enter> (numerical data may vary from this example)
```

```
aacraid 84612 8
scsi_mod 170936 10 sr_mod,usb_storage,sg,aacraid,ahci,libata,mptsa,
mptscsih,scsi_transport_sas,sd_mod
```

- To verify that the OS sees the correct CPU's are installed with the following command levels, and corresponding results:

```
cat /proc/cpuinfo | more <Enter> (complete information)
```

```
cat /proc/cpuinfo | grep -i processor <Enter> (filtered on ordered Processor numbers)
```

```
cat /proc/cpuinfo | grep -i CPU <Enter> (filtered on CPU info)
```

- To verify that the OS sees the correct amount of memory with the following command, and results:

```
cat /proc/meminfo | grep -i memtotal <Enter>
```

I.e:MemTotal: 12167900 kB

- To verify that network / Ethernet has been configured in accordance with site assigned IP Address for eth0 ONLY with the following command:

```
ifconfig -a | more <Enter>
```

- To verify that gateway has been configured in accordance with site assigned IP Address with the following command:

```
route <Enter>
```

- To verify that the default gateway can be accessed with the following command (if the ping utility is not blocked on the network):

```
ping <default gateway IP> <Enter>
```

- To verify that iLO has been configured with the site assigned static IP Address designated by the site admin, with the following command:

```
ipmitool lan print <Enter>
```

- To verify the OS version, use the following command and results:

```
cat /etc/aweos <Enter>
```

- To verify date and time-zone are correct with the following command:

```
Date <Enter>
```

3.12 HPE R/T3000 UPS (Uninterruptible Power Supply)

3.12.1 Overview

The HPE R/T3000 UPS described in this section is included in the new high-tier rack-mount version of AW Server, based on a HPE ProLiant DL580 G7 Server. The same configuration is also applicable for the HPE ProLiant DL360 Gen10 Server, HPE ProLiant DL360 Gen9 Server or HPE ProLiant DL560 Gen8 Server. For the HP ProLiant ML350 G6 Server Low Tier, no UPS offering is currently available.

Configuration of any other UPS for management of automated shutdown is beyond the scope of this document.

The initial AW Server Hardware setup, including the UPS, is the responsibility of GEHC.

When there is a UPS failure scenario, the Server Hardware vendor will be contracted to replace and / or re-configure the device back to normal.

There UPS models supported are: HPE R/T3000 G5 UPS, HPE R/T3000 G4 UPS and HPE R/T3000 G2 UPS.

Below are the details about the HPE R/T3000 G2 UPS model.

NOTE

An overview of the HPE R/T3000 G4 UPS and HPE R/T3000 G5 UPS service items is provided in [3.12.10 HP R/T3000 G4/G5 Overview on page 354](#) and detailed information is available in the HP R/T3000 G4 and G5 Service Guide 5719446-1EN, available in SIMS Content Viewer.

3.12.2 Purpose

This procedure ensures that the UPS sub-system of the AW high-tier Server is properly connected and configured to ensure a soft shutdown in case of facility power loss or disruption. This information applies to the UPS HP R3000.

This section includes valuable UPS troubleshooting, validation, and replacement procedures.

The UPS is expected to:

- Protect the server from line voltage variations and cut outs.
- Sustain server power for at least 10 minutes when utility power is unavailable.
- Shut down the HP DL580/DL560 server when utility power is still unavailable after 10 minutes.

3.12.3 How the UPS works

A rechargeable battery inside the UPS supplies continuous power to a power inverter, which converts the DC power from the battery into 50-Hz or 60-Hz power at the output of the UPS.

Under normal operation, the UPS battery is kept fully charged by AC line ("mains" or "utility") power. When AC line power is interrupted in any way, e.g., by going above or below the safe voltage range, the UPS continues to supply (using power from its battery) safe AC power for the AW Server for several minutes. This allows the AW Server to run for several minutes without line power, which should provide enough time for the users to save their data, close all exams and logoff from the AW Server, thus avoiding file corruption.

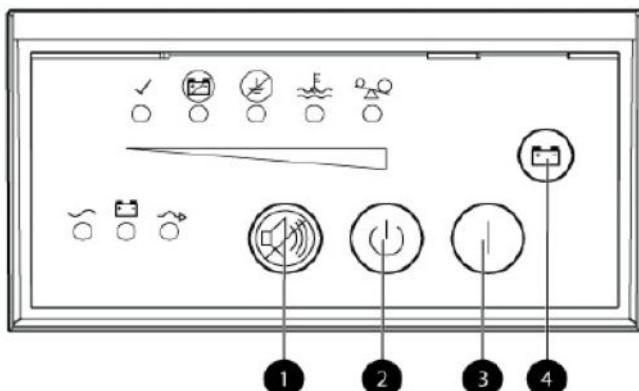
The UPS will NOT keep the AW Server running indefinitely.

3.12.4 UPS Effectivity

While this UPS may be shipped with AW Server orders, it is generally not needed and is entirely OPTIONAL when installed in the customers rack system supported by the customers own power backup scheme. It should be used when installing AW Server in an 'AW Server only' dedicated 'Stand-Alone Cabinet' configuration.

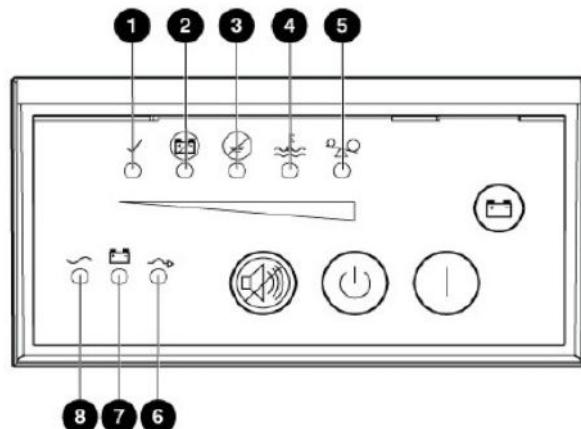
3.12.5 R/T3000 G2 Front Panel

3.12.5.1 Front Panel controls



1. Test/alarm reset button
2. Power OFF button
3. Power ON button
4. Start on battery button - when pressed with the ON button

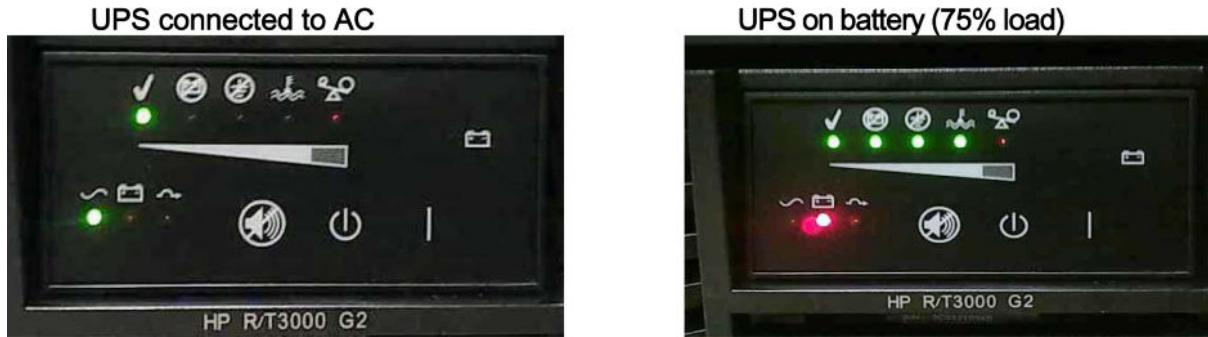
3.12.5.2 Front Panel LED indicators



1. Dual function LED : Self test and load indicator 10% load
2. Dual function LED : Battery fault and load indicator 25% load
3. Dual function LED : Site wiring fault and load indicator 50% load
4. Dual function LED : Over temperature and load indicator 75% load
5. Dual function LED : Overload and load indicator 100% load
6. On bypass indicator
7. On battery indicator
8. Utility power indicator

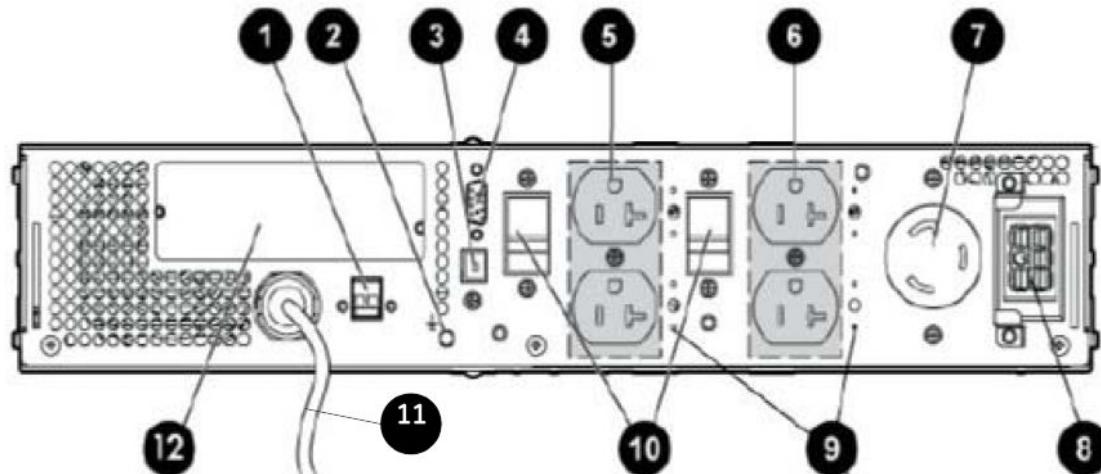
UPS connected to AC

UPS on battery (75% load)



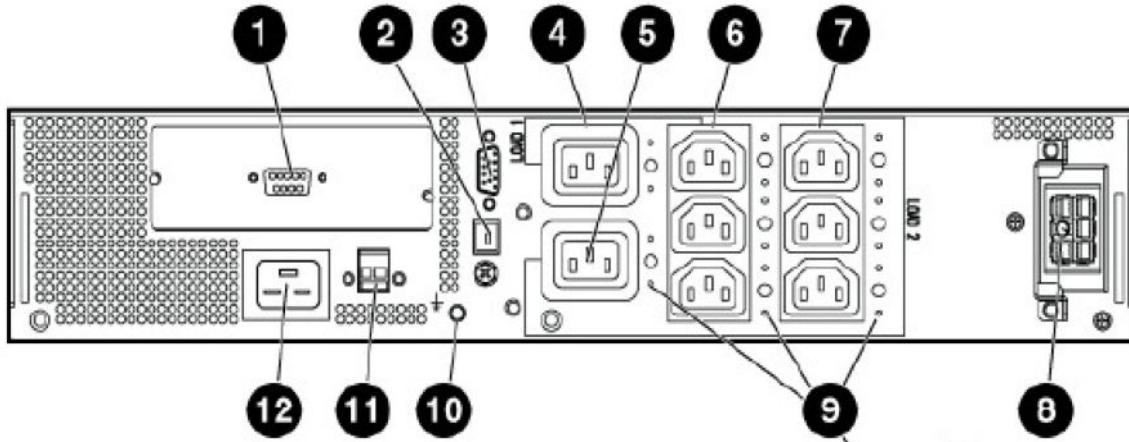
3.12.6 R/T3000 G2 Rear Panel

3.12.6.1 R/T3000 G2 US/JPN Low Voltage Rear Panel



1. REPO connector - Not used for AW Server
2. Ground bounding screw
3. USB communication port
4. Serial communication port
5. Load segment 1 (two NEMA 5-20T receptacles)
6. Load segment 2 (two NEMA 5-20T receptacles)
7. Load segment 1 - PDU output (NEMA L5-30R) receptacle - Not used for AW Server
8. ERM connection port - Not used for AW Server
9. Cable retention connection
10. Load segment circuit breakers
11. Inlet cord with L5-30P plug
12. Option slot for UPS management module - Not used for AW Server

3.12.6.2 R/T3000 G2 International high Voltage Rear Panel



- 1) UPS option card - Not used for AW Server
- 2) USB communication port
- 3) Serial communication port
- 4) and 6) Load segment 1 (1 x C19 + 3 x C13 outlets)
- 5) and 7) Load segment 2 (1 x C19 + 3 x C13 outlets)
- 8) ERM connection port - Not used for AW Server
- 9) Cable retention connections
- 10) ground bounding screw
- 11) REPO connector - Not used for AW Server
- 12) C19 inlet connection

3.12.7 Configuring the R/T3000 UPS

Drivers loading and configuration of the UPS is described in the AW Server 3.2 Installation and Service Manual, Job Card IST004A - HPE R/T3000 UPS drivers setup.

The drivers need to be loaded first from the UPS drivers CDROM, and the OS has to be loaded prior to configure the auto-shutdown feature.

Checks and safety considerations

NOTICE

Maintenance of the UPS is under the full responsibility of the Hardware Vendor. It is highly recommended that only a fully trained FE performs any required maintenance.

3.12.7.1 Checking the UPS connection to the utility power.

If the UPS is not connected to the utility power, execute the following instructions.

WARNING



To prevent injury from electric shock or damage to the equipment:

- Plug the input line cord into a grounded (earthing) electrical outlet that is installed near the equipment and is easily accessible.

- Do not disable the grounding plug on the input line cord. The grounding plug is an important safety feature.
- Do not use extension cords.

The UPS must be connected to a grounded utility-power outlet. When the UPS is plugged in, it automatically enters Standby mode and begins charging the batteries.

In Standby mode:

- No power is available at the UPS output receptacles.
- The UPS charges the batteries as necessary.

3.12.7.2 Checking the connection of the devices to the UPS

If the devices are not connected to the UPS, execute the following instructions:

NOTICE

DO NOT plug on the UPS any other equipment than AW Server related items. Do not plug laser printers into the UPS output receptacles. The instantaneous current drawn by this type of printer can overload the UPS.

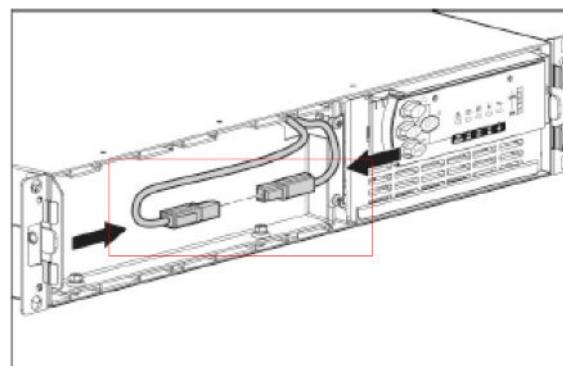
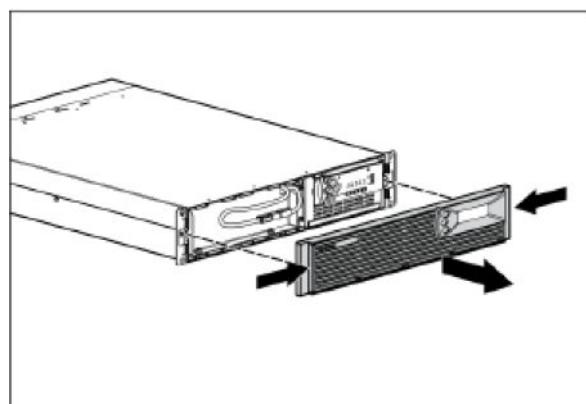
- Before connecting devices, verify that the UPS will not overload by checking that the ratings of the devices do not exceed the UPS capacity. If the equipment rating is listed in amps, multiply the number of amps by the selected output voltage to determine the VA.
- After verifying that the UPS will not overload:

Connect the device power cords to the output receptacles on the rear panel of the UPS,

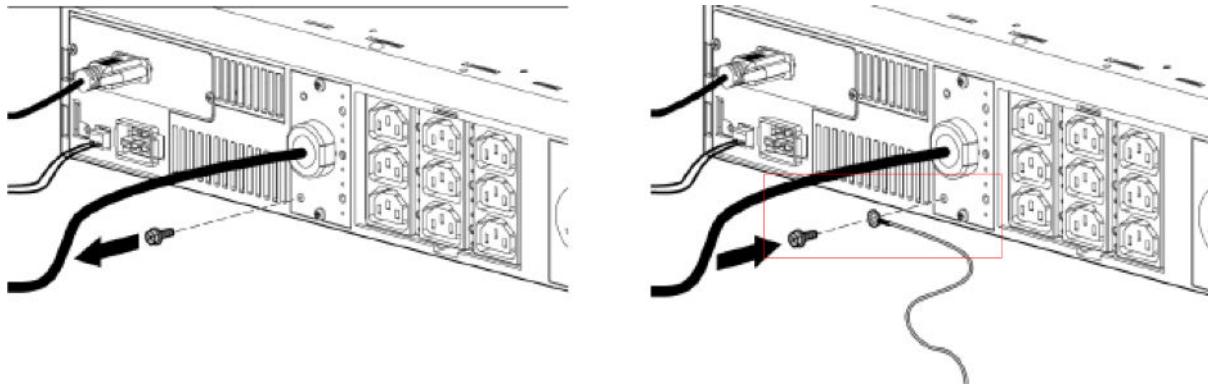
-or-

Connect devices to the output receptacles on the rear panel of the UPS using the jumper cords included with the UPS.

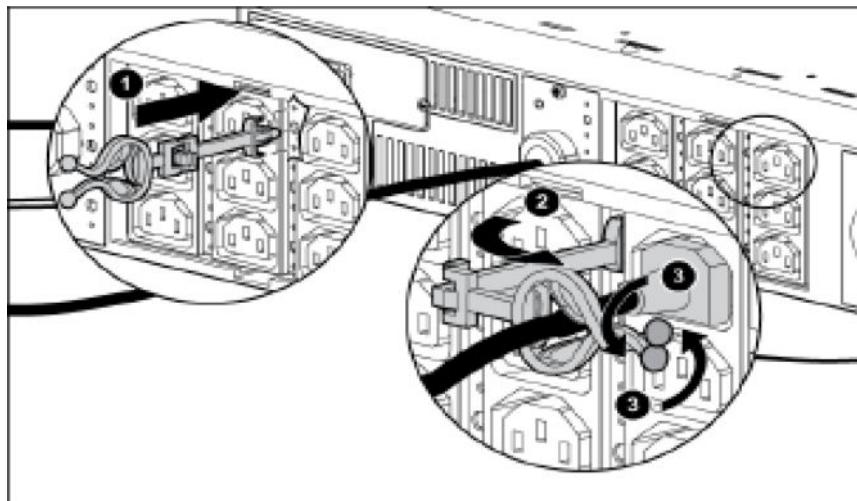
3.12.7.3 Extracting the front bezel and checking the Battery leads connection.



3.12.7.4 Checking the connection of the UPS ground bonding cable



3.12.7.5 Checking the connection of the UPS cord retention clips.



3.12.7.6 Charging the UPS batteries

Charge the batteries before putting the UPS into service.

NOTICE

Charge the batteries for at least 24 hours before supplying backup power to devices.
The batteries charge to:

- 90% of their capacity within 4 hours
 - 100% of their capacity within 24 hours

3.12.7.7 Starting power to the load

Start the power to the load by placing the UPS in Operate mode:

- Press the **On** button
- The Utility LED turns solid green indicating that power is available at the UPS output receptacles. The UPS acknowledges compliance with a short beep.

NOTE

If the UPS is using battery power (no utility power is present and the Utility LED is red), press and hold the On button until the audible alarm sounds.

If the UPS is off (no LED is illuminated), press the **On** button to start the UPS on battery power.

NOTICE

AC power must be available the first time the UPS is started.

3.12.8 Operating the UPS

This section contains the following procedures:

- Initiating a self-test
- Silencing an audible alarm
- Powering down the UPS

3.12.8.1 Initiating a self-test

To initiate a self-test, press and hold the **Test/Alarm Reset** button for three seconds.

Because a portion of the self-test requires battery power, the self-test cannot be initiated if the batteries are less than 90 percent charged. If the UPS detects a problem, the appropriate LED illuminates and an audible alarm may sound.

For information on what to do if the self-test detects a problem, see [3.12.9 Troubleshooting on page 349](#).

3.12.8.2 Silencing an audible alarm

To silence an alarm, press the **Test/Alarm Reset** button

NOTICE

Although the audible alarm silences, the condition that caused the alarm to sound may still exist. If a utility power failure caused the alarm (the Utility LED or the General Alarm LED illuminates red), the alarm silences after power is restored.

3.12.8.3 Powering down the UPS

- Shut down all load devices.
- Press the **Standby** button to take the UPS out of Operate mode. Power to the load receptacles ceases.
- Disconnect the UPS from utility power.
- Wait at least 60 seconds for the UPS internal circuitry to discharge.

3.12.9 Troubleshooting

3.12.9.1 Battery mode

When utility power is lost, the UPS automatically transfers from Operate mode to Battery mode. In Battery mode, the UPS supplies power without being connected to utility power.

When utility power becomes available, the UPS returns to Operate mode.

After the UPS is initially connected to utility power, it can be started on battery power thereafter. To start the UPS in Battery mode (no utility power present), press and hold the On and Battery Start buttons simultaneously for three seconds.

3.12.9.2 Auto-Bypass mode

The UPS automatically enters Auto-Bypass mode when one of the following conditions occurs:

- The power from the UPS reaches a percentage greater than 110 percent for more than 10 cycles or between 103 percent and 110 percent for more than 30 seconds.
- The UPS detects an overtemperature condition.
- The UPS detects a fan failure.
- There is an internal UPS failure while in Operate mode.

All internal faults transfer the UPS to either Auto-Bypass or Converter Off mode, depending on whether the load is being powered at the time the fault is detected. The UPS can be forced to Converter Off mode from Auto-Bypass mode by pressing the Off button, and can be sent back to Auto-Bypass mode by pressing the On button.

3.12.9.3 Updating the UPS firmware

To update the UPS firmware, see the HP website : <https://support.hpe.com>.

3.12.9.4 LED troubleshooting

See Section [3.12.5 R/T3000 G2 Front Panel on page 343](#)

| Utility LED | On Battery LED | On By-pass LED | Self Test LED | Battery Fault LED | Site Wiring Fault LED | Over Temp're LED | Over load LED | Condition |
|-----------------|----------------|----------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------|--|
| On - Load < 10% | Off | Off | On - Load > 10% | On -Load > 25% | On - Load > 50% | On -Load > 75% | Off | UPS is in Operate mode |
| Flashing | Off | Off | Off | * | * | * | Off | UPS is in Standby mode |
| Off | Off | On | On - Load > 10% | On -Load > 25% | On - Load > 50% | On -Load > 75% | Off | UPS is in Auto-by-pass mode |
| Flashing | Flashing | Flashing | Off | Off | Off | Off | Off | UPS in converter off mode |
| Off | Off | Off | Off | Off | Off | Flashing | Flashing | General Alarm.UPS is in Auto-bypass mode |
| On | Off | Flashing | * | * | * | * | * | Bypass is out of range |
| * | Off | * | Off | Flashing | * | * | * | Batteries disconnected or battery test failure |
| Off | Flashing | Off | Off | Off | Off | Off | Off | Low battery. No utility power |
| Off | On | Off | Battery capacity <25% | Battery capacity >25% | Battery capacity >50% | Battery capacity >75% | Off | UP is on battery. No utility power |
| * | * | * | Off | * | * | Flashing | * | Overtemperature condition |
| Off | Off | On | Flashing | Flashing | Flashing | Flashing | Flashing | Internal UPS fault |
| Flashing | Off | Off | Flashing | Flashing | Flashing | Flashing | Flashing | REPO condition |
| * | Off | * | Off | * | Flashing | * | * | Site Wiring condition |
| * | Off | * | On | On | On | On | Flashing | Overload condition
UPS capacity exceeded. No other defaults |

| Utility LED | On Battery LED | On By-pass LED | Self Test LED | Battery Fault LED | Site Wiring Fault LED | Over Temp're LED | Over load LED | Condition |
|--------------------|-----------------------|-----------------------|-----------------------|--------------------------|------------------------------|-------------------------|----------------------|---|
| * | Off | * | Off | * | * | * | Flashing | Overload condition
UPS capacity exceeded. Other defaults exist |
| Off | On | Off | Battery capacity <25% | Battery capacity >25% | Battery capacity >50% | Battery capacity >75% | Flashing | Overload condition
UPS capacity exceeded while on battery. No other defaults |
| Off | On | Off | Off | Off | Off | Flashing | Flashing | Overload condition
UPS capacity exceeded while on battery. Other defaults exist. |
| Off | Flashing | Off | Flashing | Flashing | Flashing | Flashing | Flashing | Unit is powering down |
| Flashing | Flashing | Flashing | Flashing | Flashing | Flashing | Flashing | Flashing | Checksum failure |

NOTE

*This LED can be in any state

3.12.9.4.1 UPS is in Auto-Bypass mode

The UPS transfers from Operate mode to Auto-Bypass when one of the following fault conditions is detected:

- Inverter AC over voltage
- Inverter AC under voltage
- Rectifier input over current
- Inverter output over current
- Inverter fault
- Heat sink over temperature
- Fan failure
- Overload

The load is supported, but not protected while in Auto-Bypass mode.

Troubleshooting action:

- Verify that no blockage of airflow to the front bezel and rear panel exists.
- If the condition persists, contact an HP authorized service representative.

3.12.9.4.2 UPS is in Converter Off mode

Fault conditions cause the UPS to transfer to Converter Off mode from Standby mode only. If the UPS is powering the load, fault conditions cause the UPS to transfer to Auto-Bypass mode instead. If a fault condition exists and the UPS is running in Auto-Bypass mode, press the Off button to transfer the UPS to Converter Off mode.

The load is not supported while in Converter Off mode.

The following fault conditions trigger Converter Off mode:

- Inverter AC over voltage

- Inverter AC under voltage
- Rectifier input over current
- Inverter output over current
- Inverter fault
- Heat sink over temperature

Troubleshooting action:

- Verify that no blockage of airflow to the front bezel and rear panel exists.
- If the condition persists, contact an HP authorized service representative.

3.12.9.4.3 General alarm condition

Action:

- Check the batteries
- Allow the UPS batteries to charge for 24 hours.
- If the Battery Fault LED is red, replace the batteries.
- Reduce the load:
- Power down the UPS

Troubleshooting:

- Remove one or more load devices to reduce the power requirements.
- Wait at least 5 seconds and restart the UPS.
- If the condition persists, verify that the load devices are not defective.
- Allow the UPS to cool:
- Power down the UPS
- Clear vents and remove any heat sources.
- Verify that the airflow around the UPS is not restricted.
- Wait at least 5 minutes and restart the UPS.
- If the condition persists, contact an HP authorized service representative.

3.12.9.4.4 Bypass is out of range

- The input voltage is not within ± 12 percent of nominal voltage.
- The UPS is receiving utility power that might be unstable or in brownout conditions. The UPS continues to supply power to the connected equipment. If conditions worsen, the UPS might switch to battery power.
- Bypass out of range is only a status and does not keep the UPS from transferring to Auto-Bypass mode

Action:

- Check the input voltage
- Contact a qualified electrician to verify that the utility power is suitable for the UPS.

3.12.9.4.5 Battery condition

- Check that the battery module is properly connected
- Allow the UPS batteries to charge for 24 hours..

- If the condition persists, contact an HP authorized service representative to replace the batteries .

3.12.9.4.6 UPS is on battery

Action:

- Save files and shut down connected equipment.
- Allow the UPS batteries to charge for 24 hours.

3.12.9.4.7 Input voltage is out of range

Action:

- Check the input voltage
- Contact a qualified electrician to verify that the utility power is suitable for the UPS.

3.12.9.4.8 Over-temperature condition

Possible cause: The UPS internal temperature is too high, or a fan has failed.

Action:

- Power down the UPS
- Allow the UPS to cool:
- Clear vents and remove any heat sources.
- Be sure that the airflow around the UPS is not restricted.
- Wait at least 5 minutes, and then restart the UPS.
- If the condition persists, contact an HP authorized service representative.

3.12.9.4.9 Internal UPS fault condition

Action:

- Power down the UPS
- If the condition persists, contact an HP authorized service representative.

3.12.9.4.10 REPO condition

REPO is not used for AW Server

3.12.9.4.11 Site wiring condition

Action: Contact a qualified electrician to be sure that:

- The line and neutral wires are not reversed in the wall outlet.
- A ground wire connection does not exist.

3.12.9.4.12 Overload condition

All the load LEDs are illuminated.

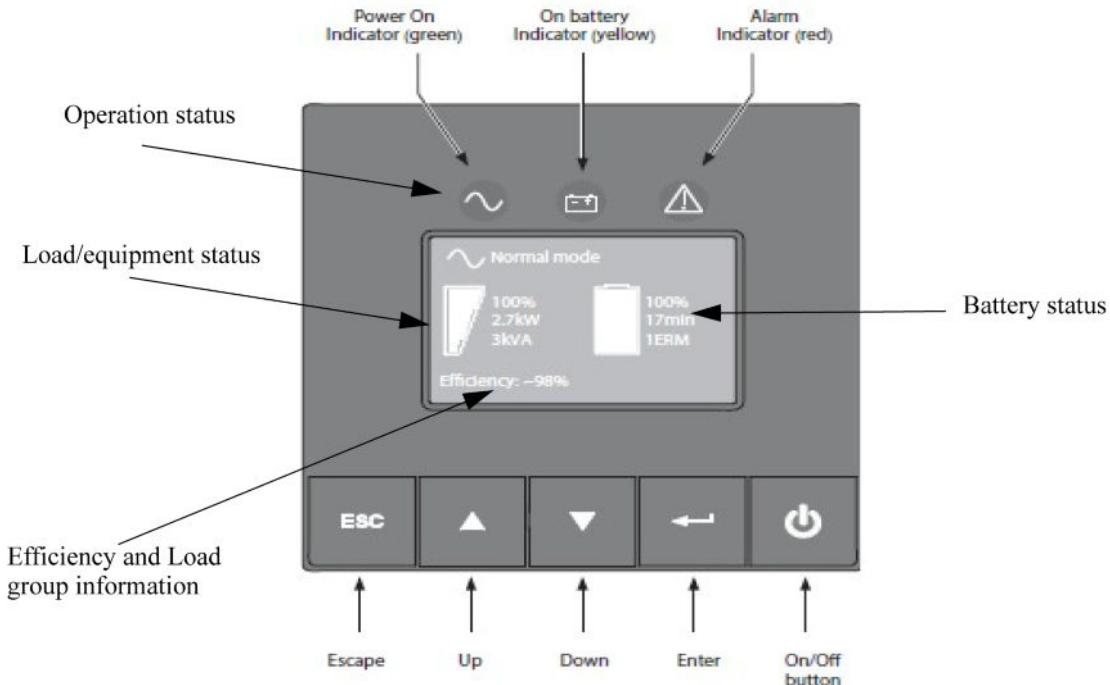
Action:

- Power down the UPS
- Remove one or more load devices to reduce the power requirements.
- Wait at least 5 seconds and restart the UPS.
- If the condition persists, verify that the load devices are not defective.

3.12.10 HP R/T3000 G4/G5 Overview

For additional details, refer to **5719446-1EN: HP R/T3000 G4 and G5 Service Guide**, available in the Service documentation.

3.12.10.1 Control panel



The following table shows the indicator status and description:

| Indicator | Status | Description |
|-----------|--------|--|
| | On | The UPS is operating normally. |
| | On | The UPS is on Battery mode. |
| | On | The UPS has an active alarm or fault. See "5.1 Troubleshooting" on page 26 for additional information. |

The LCD window provides useful information about the UPS, load status, events, measurements, and settings. As the default, or after five minutes of inactivity, the LCD displays the screen saver.

The backlight LCD automatically dims after 10 minutes of inactivity.

Press any button to restore the screen.

3.12.10.2 UPS operation

The following table illustrates the Operation Status icons that you could see and describes the condition associated with each icon.

| Operation status | Possible cause | Action |
|---|--|---|
| Standby mode
 | The UPS is off, waiting for start-up command from user. | Equipment is not powered until the  button is pressed. |
| Normal mode
 | The UPS is operating normally. | The UPS is powering and protecting the equipment. |
| In Automatic Voltage Regulation mode
 | The UPS is operating normally, but the utility voltage is outside normal mode thresholds. | The UPS is powering the equipment through an AVR device. The equipment is still normally protected. |
| No audio alarm. | | |
| On Battery
 | A utility failure has occurred and the UPS is in Battery mode.

Battery LED is on.
The audio alarm beeps every 10 seconds | The UPS is powering the equipment with the battery power.
Prepare your equipment for shutdown. |
| End of backup time
 | Battery LED is flashing.
The audio alarm beeps every three seconds | This warning is approximate and the actual time to shutdown may vary significantly.
Depending on the UPS Load and number of ERMs, the Battery Low warning may occur before the battery reaches 20% capacity. |

3.12.10.3 Troubleshooting

| Operation status | Possible cause | Action |
|---|---|--|
|  | The UPS does not recognize the internal batteries | If the condition persists, contact your service representative |
| | The batteries are disconnected | Verify that all batteries are properly connected. If the condition persists, contact your service representative. |
|  | Power requirements exceed the UPS capacity (greater than 105 % of nominal) | Remove some of the equipment from the UPS. The UPS continues to operate, but may shutdown if the load increases. The alarm resets when the condition becomes inactive. |
|  | The end of the battery life is reached. | Contact your service representative for battery replacement. |
|  | An UPS event occurs
Example:
The RPO contact has been activated to shutdown the UPS and now prevents restart. | For this event, set the contact back to its normal position and press the  button to restart. |
|  | The UPS has an internal fault | The UPS does not protect the equipment.

Note: Record the alarm message and the UPS Serial Number, then contact your service representative. |

3.13 Troubleshooting Virtual AW Server & VMware Platform

Please note that the information in this section is indicative. Exact procedures will depend on the VMware product and version used, and on the host operating system.

The installation and support of VMware products are the responsibility of the customer's IT Administrator.

3.13.1 VMware Error Messages

For assistance with error messages generated by the VMware platform, use the search tool on the VMware Support portal

<http://www.vmware.com/support.html>

You can also browse existing known problems and solutions by selecting the relevant VMware product and category Troubleshooting, for instance:

The screenshot shows the VMware Knowledge Base search interface. At the top, there's a navigation bar with links to Community, Forums, Technical Resources, Virtual Appliances, Store, and My VMware. Below that is a main menu with Cloud Computing, Virtualization, Solutions, Products, Services, Support & Downloads, Partners, and Company. The main content area is titled "Knowledge Base" and includes a search bar with the query "-VMware ESXi 5.0.x" and a dropdown set to "Troubleshooting". To the right of the search bar are buttons for "View by Article ID" and "View". Below the search bar, there are tabs for KB Articles, Product Documentation, Communities, and Wiki. On the left, there's a sidebar with sections for Narrow Focus (Products: VMware vCenter Server 5.0.x, VMware ESXi 5.1.x, VMware vCenter Server, VMware ESXi 4.1.x Installable, VMware vCenter Update Manager 5.0.x) and Activities (Using Virtual Machine, System Management, Configuring Server, Installing vSphere or Installing VirtualCenter, Using ESX). The main search results show three articles: 1. ESXi 5.0 host stops saving logs to storage (2001442), 2. Cloning a virtual machine from a template or migrating a virtual machine fails when the destination datastore is a Storage DRS POD (2021361), and 3. Cannot remount a datastore after an unplanned PDL (2014155). Each article has a rating, publication date, creation date, and last modified date. On the right side, there's a sidebar titled "Additional Resources" with sections for Alerts, Answer Wizards, Most Popular Documents, and Most Recent Documents.

3.13.2 Each VM Requires a Unique MAC Address

Normally a new MAC address is acquired as part of the VM creation process. However, if for some reason you effectively "clone" a duplicated of an existing VM, perhaps while attempting to restore a Backup VM, this will cause serious network problems. Ensure that you manually change the MAC address of a copied VM, (and be aware that you will also require a new license for the virtual AW Server, calculated using the new licenseid which is itself based on the MAC address.)

For details of how to change the MAC address of a hosted VM, refer to the VMware Knowledge Base at <http://kb.vmware.com/selfservice/microsites/microsite.do>

3.13.3 Upgrading VMware or Windows

Check with the GE OLC before installing an available upgrade to the VMware platform or Windows on the host server, as it may also require a Load from Cold of the AW Server OS and Platform.

For generic advice on upgrading VMware products, consult the VMware Knowledge Base.

3.13.4 VMware Tools - ESXi Server Compatibility

The version of VMware Tools required depends on the version of ESXi Server installed.

Note that after upgrading an ESXi Server, VMware Tools must be reconfigured on each VM.

NOTE

From AW Server 3.2 Ext. 4.0, the Open VM Tools (open source implementation of VMware Tools) are installed as part of the OS. Installing the VMware Tools is not needed.

3.13.5 Ensure VMware Tools Configured for Graceful Shutdown

NOTE

For a virtual AW Server, ensure that VMware Tools is configured to execute a graceful shutdown of the guest operating system occurs:

For a VMware hypervisor, ensure that VMware Tools are installed and running. Do not skip this step, otherwise the VMware tools will not be considered as installed and you won't be able to use the guest shutdown shortcut:

- **vSphere Client case:**

- Select the Virtual Machine and check that in the summary panel the VMware Tools are indicated as "**Running**".

NOTE

If it is not the case, install the VMware Tools prior to continue with the next steps.

- Click on the



Shut Down Guest button.

The following message should display:

Shutdown the guest operating system of the virtual machine 'AWS3_VM01'?

Click on **No** unless you want to shutdown your Virtual Machine.

- **vSphere Web Client case:**

- Select the Virtual Machine and check that the



Shut down button is available.

NOTE

If the button is not available, contact the site IT admin to install the VMware Tools prior to continue with the next steps.

NOTE

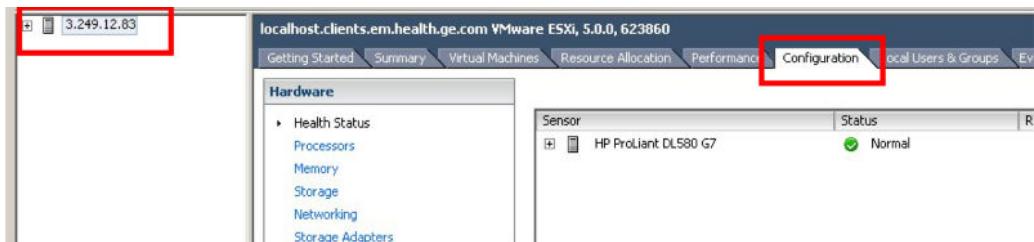
For further details, refer to the AW Server 3.2 Installation and Service Manual, Job Card IST004B - Installation of VM Tools.

3.13.6 Ensure VMware Hypervisor Configured with Same NTP Server as AWServer VM

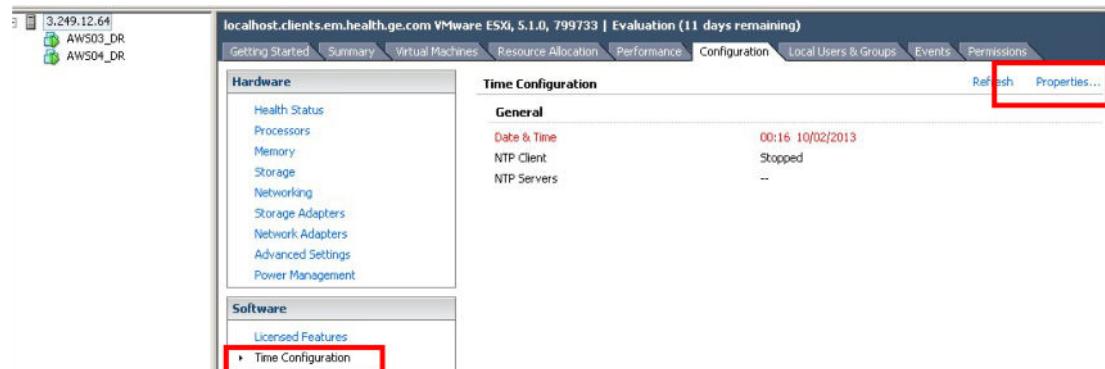
The ESXi server must be configured to use the same time server as that used by its AW Server VMs.

3.13.6.1 Setup a NTP server for the ESXi server

1. Make sure you are logged on the vSphere Client as **root**.
2. • Select the Hypervisor and click on the **Configuration** tab.



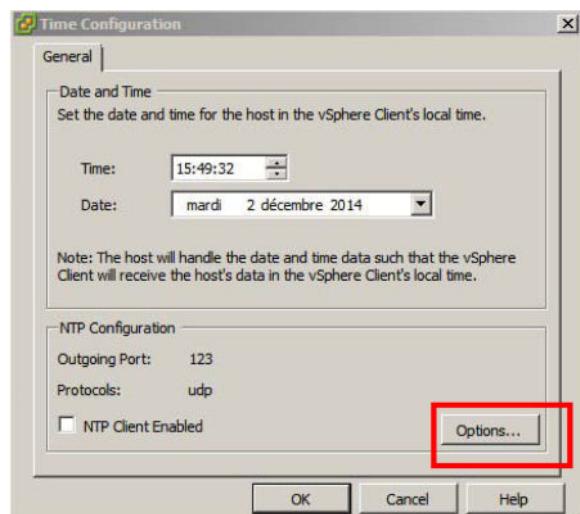
3. • Click on **Time configuration** under **Software** category.



- Click on **Properties** on the right side of the screen.

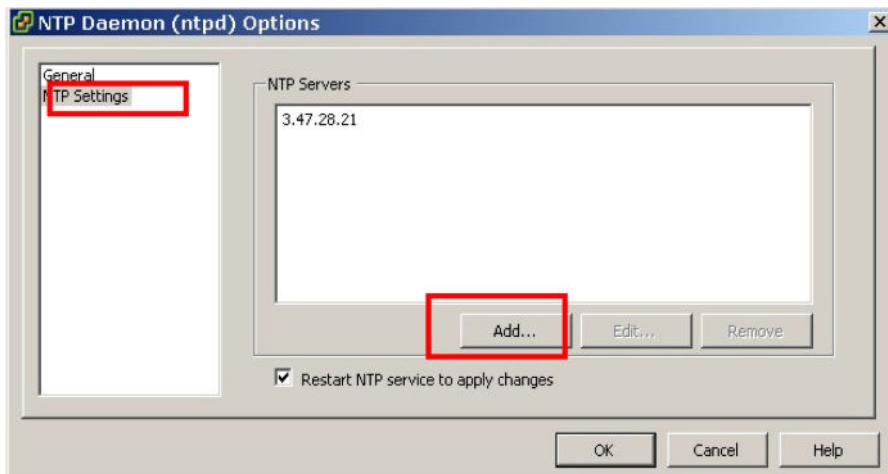
4. The Time Configuration screen displays.

- Click on **Options**.

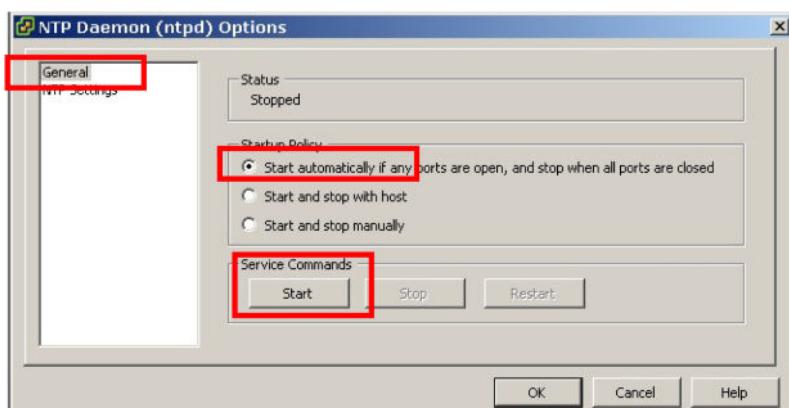


5. The NTP Daemon Options screen displays.

- Click to select **NTP Settings**.



- Click on the **Add** button and enter the site's NTP server name (I.e: *ntp.pool.org*) or NTP server's IP address in the "Add NTP Server" popup window, then click on **OK** when done.
- 6. • Click back to select **General** and set the startup Policy to Start automatically.



- Start the NTP service by clicking on the **Start** button
- 7. Verify that the NTP service has been started and is running.

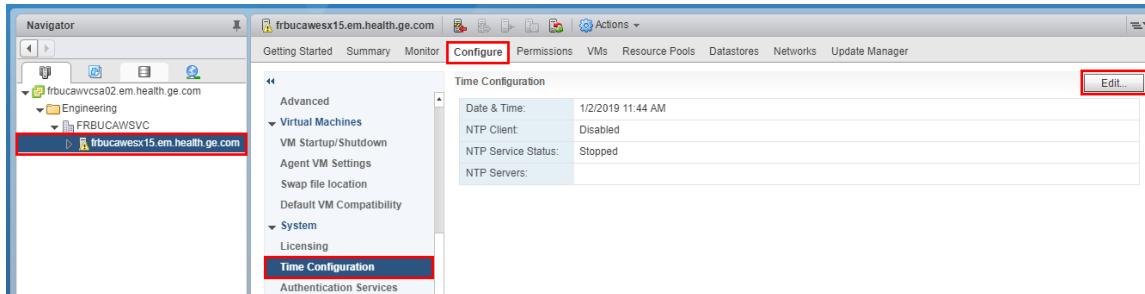


- 8. The GEHC FE shall be provided with the IP address of the NTP server that was used, so that he will be able to set it in the Virtual AW Server once installed.
This completes the installation of a NTP server for the ESXi server.

3.13.6.2 vSphere Web Client case

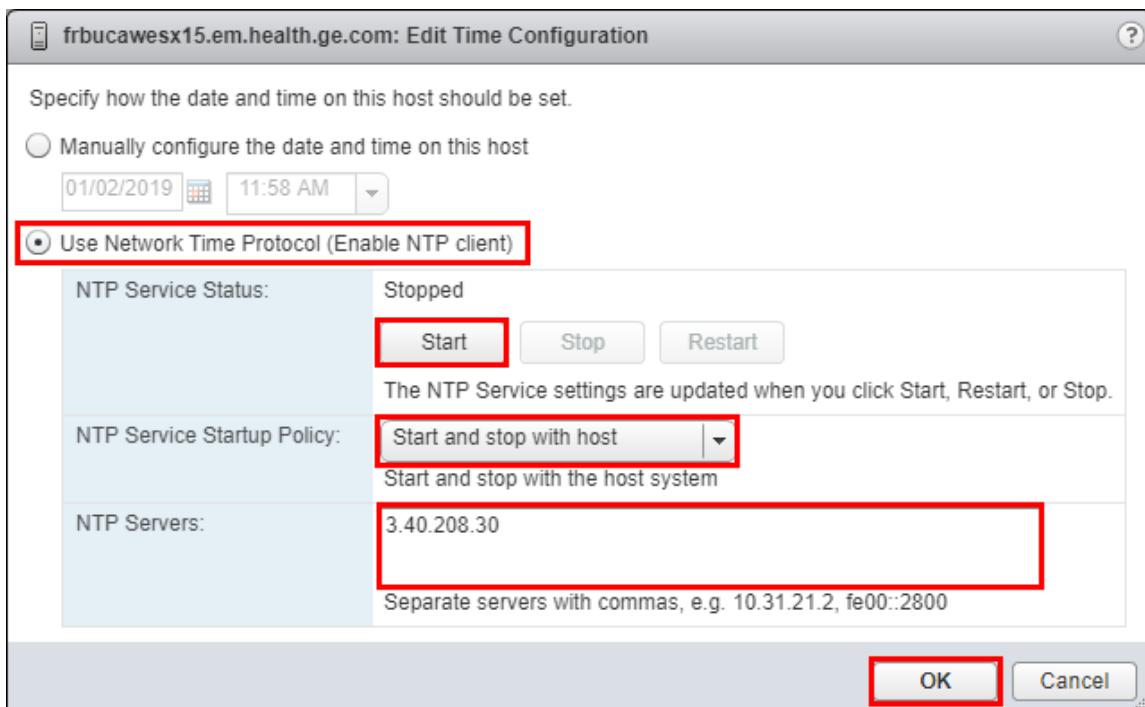
1. Make sure you are logged on the vSphere Web Client as **administrator**

2. In the main vSphere Web Client screen:



- Select the Hypervisor and click on the **Configure** tab.
 - Expand **System** sub-menu and click on **Time Configuration**
 - Click on **Edit** button.
3. Configure and start the NTP server.

In the *Edit Time Configuration* screen that displays:



- Select **Use Network Time Protocol (Enable NTP client)** radio box.
- Enter the site's NTP server name (I.e: *ntp.pool.org*) or NTP server's IP address in the **NTP Servers** field.
- Set the **NTP Service Startup Policy** to **Start and stop with host**
- Start the NTP service by clicking on the **Start** button
- Click on **OK** button to complete the NTP server installation.

4. Verify that the NTP service has been started and is running.

| Time Configuration | |
|----------------------------|-------------------|
| Date & Time: | 1/2/2019 12:27 PM |
| NTP Client: | Enabled |
| NTP Service Status: | Running |
| NTP Servers: | 3.40.208.30 |

5. The GEHC FE shall be provided with the IP address of the NTP server that was used, so that he will be able to set it in the Virtual AW Server once installed.

This completes the installation of a NTP server for the ESXi server.

3.13.7 Windows Memory Management

In some cases the hard disk on the Windows host may become full and/or VMware operations may fail.

To avoid this risk, configure Windows memory management as follows:

1. Review the size of the Windows swapfile (pagefile.sys)

Go to **Control Panel > System > Advanced System Settings > Performance Settings > Advanced > Virtual Memory**. Set it to "custom size" and select a size (in MB).

Ensure that it is set to the recommended memory setting or higher. (Likely to be equivalent to the total amount of physical RAM installed)

2. Eliminate the hiberfile.sys file

Execute the following command at the command prompt, in Administrator mode:

`powercfg -h off <Enter>`

Reboot the system to take the new settings into account.

3.13.8 Limitations of Virtual AW Server

Limitations of the AW Server product related to virtualization include the following:

- iLO is not available for virtual AW Servers.
- On the Service Tools > Healthpage, some fields return Not applicable or blank values, others return the value of virtualized hardware rather than physical hardware.

3.13.9 Virtual disk for images is too small

Problem: The virtual disk used to store images is too small. For example, the virtual disk was created with a size of 100GB only at installation time, and there is no more free space.

Solution: A possible solution is to expand the size of the virtual disk in VMware. Once this is done, it will also be needed to erase the image partition on the AWS and create a new one.

NOTICE

All images will be lost during this procedure. Ensure that all images are backed up.

- Steps to perform in VMware:
- Login to VMware vSphere Client.
- Edit the settings of your Virtual Machine.
- Select the second virtual disk. In "provisioned size", enter a bigger size.
- Select OK to apply the changes.

The size of the second virtual disk has now been expanded. However on AWS side, the guest OS still has an image partition with the previous smaller size.

- Steps to perform on AW Server:
- Perform a Load From Cold as described in the AW Server 3.2 Installation and Service Manual.
- During the Load From Cold, when the installer asks if image partition shall be kept, select "Erase". The installer will create a new image partition, using all the space on the virtual disk that you expanded.
- After installation, use the command `df -h <Enter>` to check the size of the image partition.

3.14 Troubleshooting An Integrated Server

3.14.1 Troubleshooting hybrid integration

When encountering issues with hybrid integration, perform the following checks:

- Test the AW Server Client connection to AW Server. If this is working, the issue can probably be isolated as a hybrid integration issue.
- Check connectivity between the different components: AW Server, Client PC, PACS.
- Check that the path to integration.exe is correct in PACS Client configuration files.
- Check all items on the checklist provided in AW Server 3.2 Installation and Service Manual, Job Card IST011 - Integration.

3.14.2 Connectivity Limitations in Seamless Integration Mode

The remote connectivity (InSite/RSvP) solution is not used by GEHC IT and is therefore not configured on AW Server in Seamless Integration Mode with Universal Viewer client. This results in the following limitations:

- Prodiags is not available.
- Problem Report tools (version prior to AW Server 3.2 Ext. 4.2) will not send data to the GE Back Office.
- If you want to use an SSH port for remote connectivity you will have to manually enable it. See [3.4.5.4 SSH \(Secure Shell\) on page 188](#).

3.14.3 Troubleshooting Seamless Integration

In case of issues with Seamless Integration, for example when the 3D Applications button of the Universal Viewer Client is greyed out, apply one or both of the following procedures before considering other solutions:

1. Use the checklist provided in the AW Server 3.2 Installation and Service Manual to ensure that all components have been correctly configured and installed. This checklist covers all components used in seamless integration: AW Server, Universal Viewer Server, Universal Viewer

Client PC and image sources. For each item in the checklist, you can refer to the indicated section of the AW Server service documentation. You can also use the Universal Viewer Installation Manual for additional information.

2. If possible (check with the customer), reboot / restart the following :
 - a. Reboot AW Server.
 - b. Restart Universal Viewer services (see Universal Viewer documentation)
 - c. Reboot Universal Viewer Client PC (perform a Windows restart)

After these reboots are all complete for all systems, retry the operations where you encountered the original issue.

3.14.4 End of Review Setting Lost When Switching Between Full & Seamless Integration

End Of Review must be configured for PACS integration, so that processed data is automatically pushed to the remote system (PACS). Note that only generated data will be sent.

End of Review configuration is lost when you switch between Full and Seamless Integration. If you change the integration mode, re-configure End of Review. (The desired Integration must be fully configured **prior** to configuring End Of Review.

3.15 Troubleshooting AW Server Clusters

3.15.1 Single Access to All AW Server Logfiles in a Cluster

When a number of virtual servers are configured as a scalable cluster, the number of clients and corresponding logfiles increases accordingly.

To simplify access to all the AWServer logfiles of a cluster, the `cluster_mount_logs.sh` script is provided. The following procedure explains how to use it and the resulting logfile collection.

- Login to Service Tools on one of the cluster nodes as `root`.
- Select **Initial configuration > Scalability** and note the correspondence, for each of the nodes, between ip addresses on the hospital and private networks (for instance by taking a screen snapshot).



- Select **Tools > Terminal**

- Login as root.
- Check the logfiles

```
cd /usr/share/ServiceTools_AWS/scripts/nfs <Enter>
```

```
./cluster_mount_logs.sh <Enter>
```

- To locate the root logfile directory on the mount, for a given node, type:

```
cd /mnt/log/<private ip> <Enter>
```

(where *<private ip>* is the ip address on the private subnet that corresponds to the node in question).

```

Login: root
Password:
Last login: Thu Mar  7 17:42:13 2013 from localhost
awsvc10:~ # /usr/share/ServiceTools_AWS/scripts/nfs/cluster_mount_logs.sh
Querying cluster node list.
Found 4 nodes in the cluster.

==== 192.168.0.4 ====
Mounting 192.168.0.4:/var/log under /mnt/log/192.168.0.4

==== 192.168.0.3 ====
Mounting 192.168.0.3:/var/log under /mnt/log/192.168.0.3

==== 192.168.0.2 ====
Mounting 192.168.0.2:/var/log under /mnt/log/192.168.0.2

==== 192.168.0.1 ====
Mounting 192.168.0.1:/var/log under /mnt/log/192.168.0.1

awsvc10:~ # cd /mnt/log
awsvc10:/mnt/log # ls
192.168.0.1 192.168.0.2 192.168.0.3 192.168.0.4
awsvc10:/mnt/log #
```

- To access the sub-directory containing the client logfiles, type:

```
cd gehc/sdc/logfiles <Enter>
```

NOTE

For each node, the `/mnt/log/<private ip>/gehc/sdc/logfiles` directory is a mounted partition to the `/var/log/gehc/sdc/logfiles` directory on the cluster node.

You can of course navigate manually through the logfiles on the mount via the terminal window, and open or copy them as required.

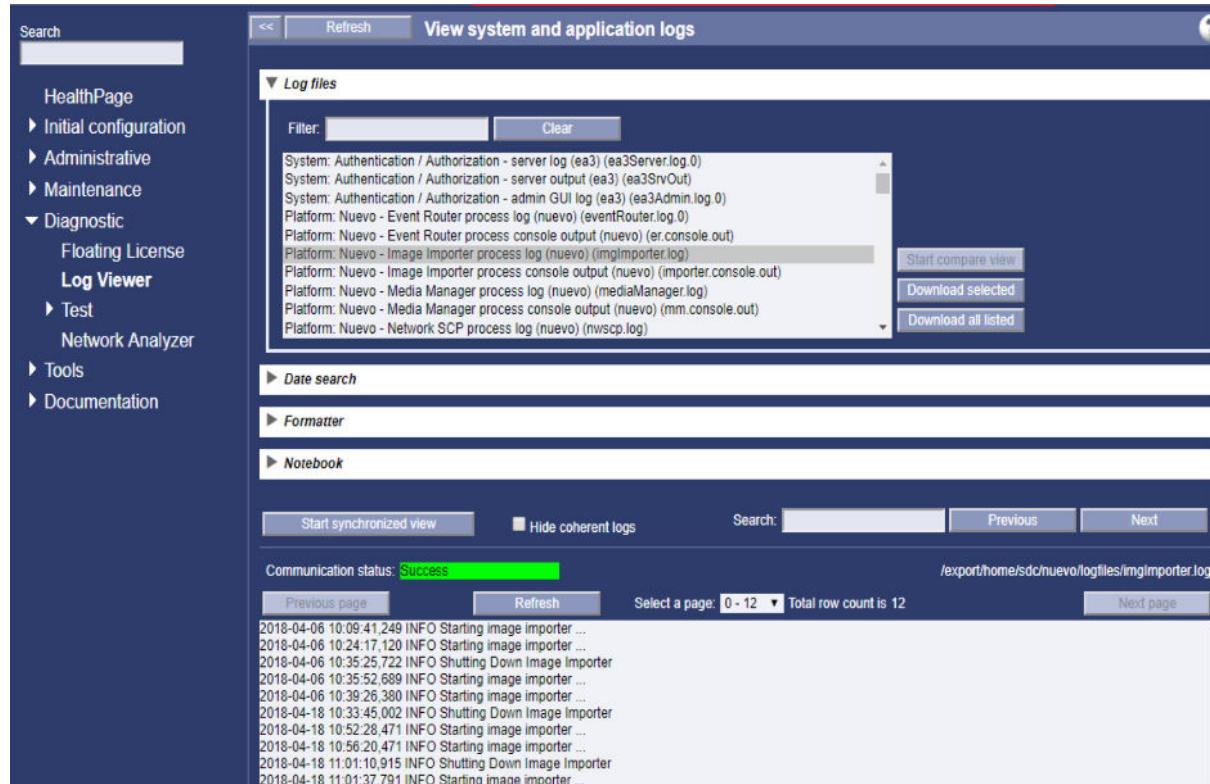
It is easy to navigate to all logfiles of the AWServers from the mounted partitions under `/mn/log/` using the terminal and UNIX commands like a recursive grep.

There is no central location for all client logfiles. You must first identify on which node the log file of the client is stored. Then, you can log on the appropriate server and use the Log Viewer in the Service Tools.

You can use this tool to filter, analyze and/or download the files. (Further details of this tool are given in [3.2.3 Log Files Viewer on page 126](#) of this chapter.)

- Select **Diagnostic > Log viewer**

The client logfiles are prefixed with `Client:` (at the bottom of the list in the top pane of the Viewer).



- Select one to view its contents in the bottom pane of the Viewer.

To download some or all of these logfiles, select them then click **Download selected**.

NOTE

Always use FFA tool to download files remotely.

- Click **OK** to acknowledge the file size message, then select **Open** or **Save**.

The file collection will be downloaded in a compressed file named `logfiles_<date_time_stamp>.zip`

- When you have finished working with the client logfiles, close the mount:

Type: `cd /usr/share/ServiceTools_AWS/scripts/nfs <Enter>`

Type: `./cluster_umount_logs.sh <Enter>`

NOTE

If the unmount fails, you can force it by identifying the process using the mount and killing it manually, before relaunching it:

Type: `lsof /mnt/log/<private ip>/ <Enter>`

Note the returned PID (Process Id)

Type: `kill -9 <PID> <Enter>`

(where <PID> corresponds to the numeric PID)

Type: `./cluster_umount_logs.sh <Enter>`

After killing the process, try to execute the umount script again.

3.15.2 Number of login allowed in a cluster

In an cluster of AW Servers, the number of concurrent login allowed is determined by the application licenses installed in the Floating License Server. This limitation is not impacted by the number of AW Server nodes in the cluster, as it is only related to the Floating License configuration.

For example, if the Floating License server declared for the AW Server nodes has a Volume_Viewer license for 10 concurrent users, it will not be possible to launch Volume Viewer application for 11 users. The last (in this case, 11th) user trying to launch Volume Viewer will see a pop-up indicating that all Volume_Viewer license tokens are already in use.

Another limitation comes from the maximum number of slices that can be manipulated by an AW Server. For each AW Server, the platform license determines how many slices can be opened by this AW server: 8,000, 16,000, 40,000, 80,000 or 160,000 slices depending on the platform license. This limitation is impacted by the number of AW Server nodes in the cluster.

3.15.3 Troubleshooting HAPS nodes

HAPS nodes are machines dedicated to preference sharing management, only used for cluster of AW Servers.

A HAPS node uses the same OS as the AW Server node, however it does not run the AW Server platform. Instead, a HAPS node runs a shared filesystem used to store and share preferences, (called *glusterfs*).

For each cluster of AW Servers, there should be two HAPS nodes. Only one HAPS node is needed to manage the preferences, the other HAPS node is used as a backup if the first node fails, providing high availability.

When troubleshooting HAPS nodes, use the following tools:

- **Scalability page from Service Tools**

Login to the Service Tools of an AW Server node. Display the **Initial Configuration>Scalability** page. This page contains information on the two HAPS nodes: status, IP addresses, free space... Use this information to diagnose the current state of the two HAPS nodes.

- **Remote access to HAPS node**

If you need to run command lines on the HAPS node, use an ssh client (e.g. putty) and connect to the HAPS node public IP address through ssh.

NOTE

Service Tools are not running directly on the HAPS node. You can see HAPS node status in the Service Tools of AW Server nodes.

When encountering issues with HAPS nodes, check the following :

- For all AW Server nodes, IP addresses entered in *Initial Configuration > Platform Configuration > Scalability* tab are the private IP addresses of HAPS nodes.
- On any AW Server node, check the status of HAPS nodes in *Initial Configuration > Scalability* page.
- If one HAPS node is not available, check the network connection between HAPS node and AW Servers nodes, using ping.
- If one HAPS node is not available but connectivity is working, connect to the HAPS node through ssh and use one of the following command:
 - **gluster pool list <Enter>**
This will display a list of the HAPS nodes and their status
 - **gluster volume status <Enter>**
This will display the status of the preferences "folder" (also called volume).
 - **service glusterd status <Enter>**
This will display the status of the glusterd service which is needed for HAPS to run.
 - **service glusterd restart <Enter>**
This will restart the service for sharing of preferences. Only perform this step if the HAPS node presents an error. If AW Server nodes are not in Maintenance Mode, this could impact customer activity.

3.16 Troubleshooting Client Software

3.16.1 AW Server Client Logfiles

The Windows version of the AW Server Client creates logfiles which are stored in the user's Application Data folder, for example

C:\Users\<Windows User>\AppData\Roaming\Solo\<Session id>\logs

or

D:\Documents and Settings\<Windows User>\Application Data\Solo\<Session id>\logs

These logfiles are in text format and contain useful data about file and process usage by session.

3.16.2 AW Server Client supported monitor

AW Server supports identical horizontally aligned dual monitor clients with a recommended combined resolution of 4MP (2x2MP), larger monitors may be used. Advanced applications may take advantage of the dual screen support to allow larger or more numerous views.

AW Server cannot be configured in two screens mode if the monitors have different horizontal screen resolution.

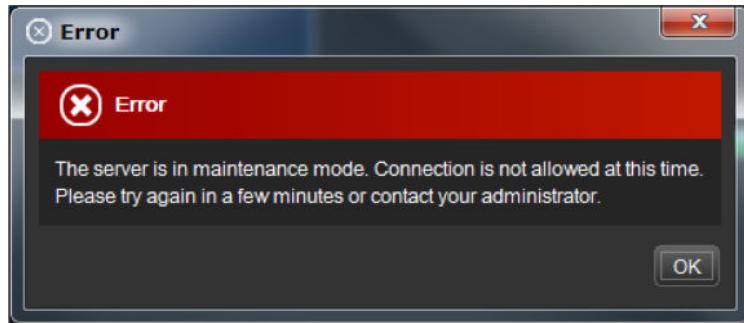
3.16.3 Known error messages for AWS Client

3.16.3.1 Maintenance Mode Error message

Error message:

When logging in to AW Server Client, the following error message is displayed:

"The server is in maintenance mode. Connection is not allowed at this time. Please try again in a few minutes or contact your administrator."



Cause:

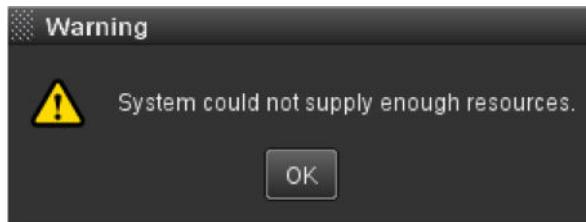
This message is displayed when the AW Server is in Maintenance Mode. You can check the status of Maintenance Mode using the Service Tools. Remember that once an AW Server is put in Maintenance Mode, it will not leave this mode even after a reboot. Use the finish Maintenance Mode menu to allow AW Server Client connection again. Refer to Chapter 4, [4.2 Maintenance Mode on page 388](#)

3.16.3.2 Resources Error message

Error message:

When launching an application in the AW Server Client, the following message displays:

"System could not supply enough resources."



Possible cause:

This message can be displayed if no platform license key has been configured. To check this, log in to the Service Tools, and display the **Initial Configuration>Platform Configuration** menu. If there is no key entered in the Platform License key, follow instructions in Chapter 2, [2.3.8 Platform Configuration on page 62](#) to configure it.

If there is a platform key configured, this message might be caused by incorrect hardware configuration. Use the Service Tools Healthpage to display Hardware status, and check if there are any specific hardware requirement for the application you are using.

This error message could also appear in combination with the following one when trying to launch an application from the AW Server Client. Please refer to [3.16.3.3 Display configuration error when trying to launch an application on page 368](#) for troubleshooting.

3.16.3.3 Display configuration error when trying to launch an application

Issue:

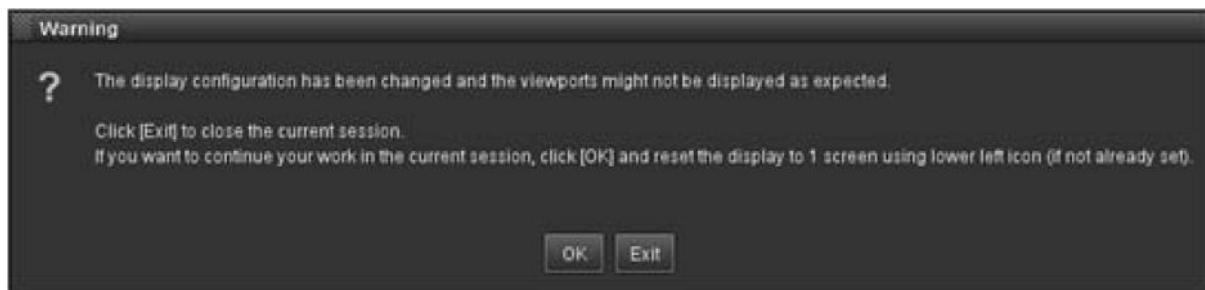
When launching an application in the AW Server Client, the following message displays:

The display configuration has been changed and the viewports might not be displayed as expected.

Click on [Exit] to close the current session.

If you want to continue your work in the current session, click on [OK] and reset the display to 1 screen using lower left icon (if not already set).

It might appear in combination with the previous error message after an upgrade from a previous version of AW Server.



Possible cause:

In case of upgrade from a previous version of AW Server, a preference file containing outdated information (from previous version) might be restored.

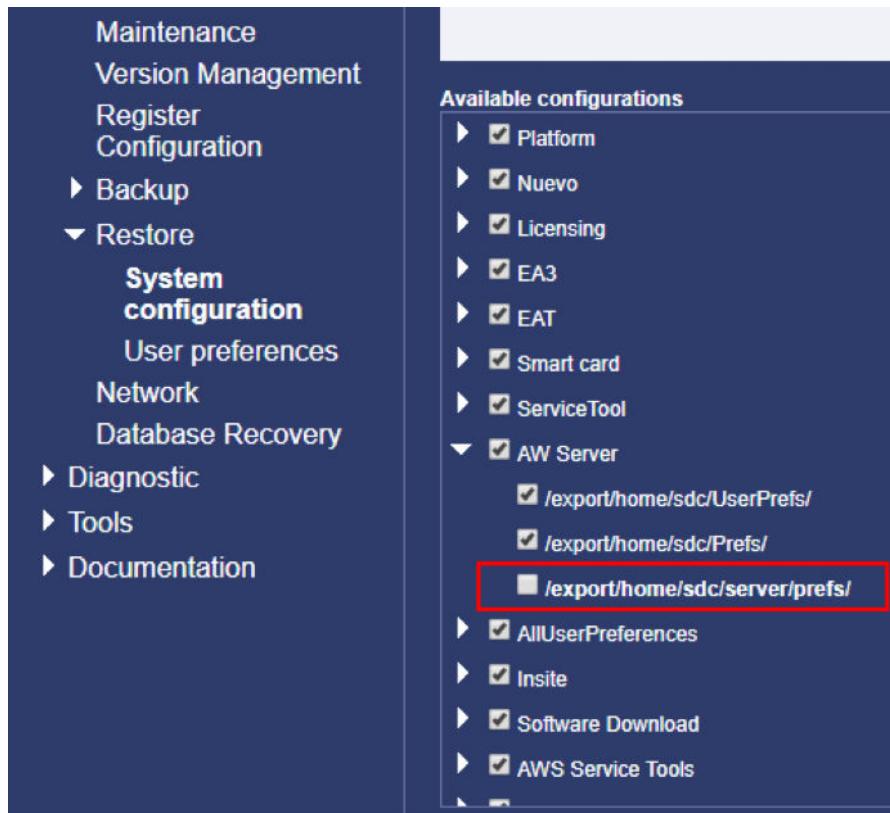
Solution:

- To fix this issue, you must correct this file that was imported from a previous version of AW Server.
 1. Note down the parameters for End Of Review as you will have to reconfigure it at the end of the procedure.
 2. Check whether the ServerPreferences.properties file contains incorrect information:

```
cd export/home/sdc/server/prefs/ <Enter>
grep version ServerPreferences.properties <Enter>
```
 3. If the output refers to an older version of AW Server (i.e. aws-2.0 as indicated below), then you must replace the file:

```
/com/ge/med/awe/preferences/version=aws-2.0-12.0
```
 4. Create a backup copy of this file and replace it by the .original file as instructed below:

```
cp ServerPreferences.properties ServerPreferences.properties.old
<Enter>
cp ServerPreferences.properties.original ServerPreferences.properties
<Enter>
```
 5. You must de-install then re-install the advanced applications (especially Volume Viewer).
 6. Reconfigure End Of Review (refer to AW Server 3.2 Installation and Service Manual for the procedure).
- If the problem persists or if you cannot perform the steps described above, then you must perform a Load From Cold of the AW Server OS and Platform and chose to restore all the files except the incorrect Server preferences:



Refer to the AW Server 3.2 Installation and Service Manual for the detailed procedure.

3.16.3.4 Windows file and folder access needed to run AWS Client

In order to run the AWS Client, the Windows user needs permissions to:

- write in directory %APPDATA%\Solo
- write in directory %USERPROFILE%\ .solo
- write the file %USERPROFILE%\ .AWEtruststore

The Windows user also needs permissions to read and execute the following programs from the AWS client installation folder:

- solo.exe
- nxproxyGEAWE32.exe
- integration.exe

3.16.3.5 "Another version of this product is already installed"

Issue: When installing the AW Server Client, the following message displays:

"Another version of this product is already installed. Installation of this version cannot continue. To configure or remove the existing version of this product, use Add/Remove Programs on the Control Panel."

Root cause: It is not possible to have two different minor releases of AW Server Client on the same system. For example, it is not possible to install AW Server 3.2 and AW Server 3.2 Ext. 2 clients on the same system.

Solution: You first need to remove the other AW Server Client version, as described in [5.5.1.1 AW Server Client upgrade Procedure on Windows on page 433](#) or [5.5.1.2 AW Server Client for Universal Viewer upgrade Procedure on page 436](#)

NOTE

It is possible to install different AW Server Client major releases on the same system, for example AW Server 2.0, AW Server 3.0, AW Server 3.1 and AW Server 3.2 clients. It is also possible to install both AW Server 3.2 client and AW Server 3.2 client for Universal Viewer on the same system.

3.17 Troubleshooting disk encryption

HDD replacement: No secure encryption-related steps are associated with this case. Follow the usual HDD replacement procedure. No additional action is needed. The newly installed HDD will be automatically encrypted. The data on the removed HDD will be unreadable if the Master Encryption Key is not known.

Motherboard replacement: Follow the usual motherboard replacement procedure. Then, follow section [3.17.5 Configuring the Smart Array Controller for Local Key Management Mode on page 375](#).

Smart Array Controller replacement: If some or all the drives managed by the controller being replaced are encrypted, you must re-configure the replacement controller with the same settings and key management mode used for the original controller. Follow sections [3.17.8 Replacing an Encrypted Smart Array Controller on page 378](#) and [3.17.5 Configuring the Smart Array Controller for Local Key Management Mode on page 375](#). Define the same Master Encryption Key as used on the original controller. If a different Master Encryption Key is defined, the server can't boot and must be reinstalled from scratch.

Other Server FRU replacement: No encryption-related tasks to complete. Apply the usual FRU replacement procedure.

Lost or forgotten Crypto Officer Password, Master Encryption Key or Password Recovery Answer: Follow sections [3.17.6 Recovering the Crypto Officer Password on page 377](#) or [3.17.7 Lost or forgotten Master Encryption Key on page 378](#) or [3.17.9 Changing the password recovery settings on page 378](#). Then follow sections [3.17.3 Clearing a Smart Array Controller on page 373](#) and [3.17.5 Configuring the Smart Array Controller for Local Key Management Mode on page 375](#). Reconfigure the system using a new Master Encryption Key.

Replacing a server while retaining the controller: If you retain the same controller and physical disks, then there are no encryption-related tasks to complete.

3.17.1 Accessing Encryption Manager

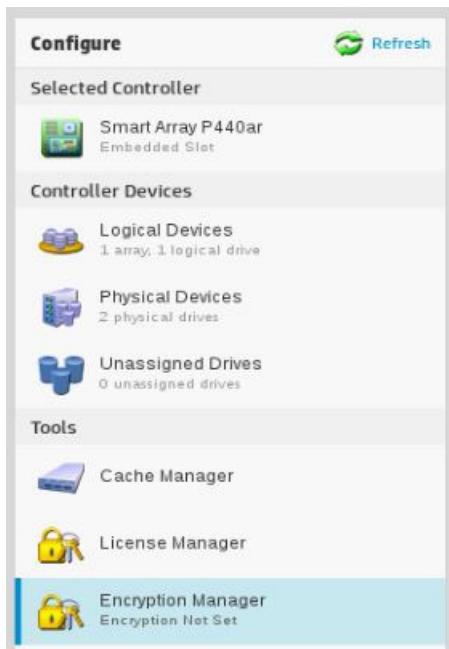
The HPE Smart Storage Administrator (HPE SSA) is a configuration and management tool for HPE Smart Array controllers. See the AW Server 3.2 Hardware Installation Manual for details to start the HPE Smart Storage Administrator (HPE SSA). For additional information, see the HPE Smart Storage Administrator User Guide.

1. To open the Encryption Manager, start HPE Smart Storage Administrator (HPE SSA).
2. Select a Secure Encryption-compatible controller.

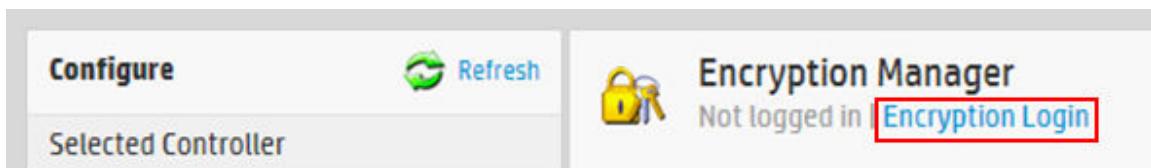


3. Click on **Configure**.

4. Under **Tools**, click on **Encryption Manager**.



5. Click on **Encryption Login**.



A new window appears.

6. Select **Crypto Officer** and enter the Crypto Officer password in the **Password** field provided.

The screenshot shows the 'Encryption Login' window. At the top, it says 'Encryption Manager Not logged in > Encryption Login'. Below that, under 'My Account', 'Crypto Officer' is selected. In the 'Password' section, there is a text input field labeled 'Please enter password:' and a 'Show' link next to it.

7. Click on **OK** to continue.

The *Settings* page appears.

3.17.2 Clearing Encryption Configuration

Important

Clearing all encryption settings clears all secrets, keys, and passwords from the controller. Secure Encryption will be returned to a factory-new state.

1. Clear the controller.

See [3.17.3 Clearing a Smart Array Controller on page 373](#).

Important

Clearing the controller is not necessary if there are no encrypted drives present or if HPE Smart Storage Administrator (HPE SSA) is operating in an offline mode.

2. Access the Encryption Manager.

See [3.17.1 Accessing Encryption Manager on page 371](#).

3. Under *Utilities*, click on **Clear Encryption Configuration**.

A prompt appears indicating all encryption settings will be cleared from the controller.

4. To continue, click on **Clear**.

3.17.3 Clearing a Smart Array Controller

Clearing a Smart Array Controller deletes the existing arrays or logical drives, and any data on the logical drives. Before proceeding, backup the AW Server configuration as described in the AW Server 3.2 Installation and Service Manual, Job Card UPG001 - Software Upgrade.

To clear a Smart Array Controller:

1. Start HPE Smart Storage Administrator (HPE SSA).
2. Select the controller to be cleared.

3. Under Actions, click on **Clear Configuration**.

The screenshot shows the 'Configure' screen for the selected controller. The left sidebar lists 'Controller Devices' (Logical Devices: 2 arrays, 2 logical drives; Physical Devices: 8 physical drives; Unassigned Drives: 0 unassigned drives) and 'Tools' (Cache Manager, License Manager, Encryption Manager). The right panel displays the 'Actions' section for the 'HPE Smart Array P408i-a SR Gen10' controller in the 'Embedded Slot'. The 'Actions' section includes buttons for 'Modify Controller Settings', 'Set Sanitize Lock', 'Advanced Controller Settings', 'Modify Spare Activation Mode', and 'Clear Configuration'. The 'Clear Configuration' button is highlighted with a red border.

A new window appears confirming your request to clear the controller's configuration.

4. To continue, click on **Clear**.

The screenshot shows a confirmation dialog box titled 'Clear Configuration' for the 'HPE Smart Array P408i-a SR Gen10' controller. The message area contains the following text: 'Clearing the configuration of the selected controller will delete all of its arrays and logical drives! All data on the logical drives will be lost! Any operations currently queued or in progress on logical drives will be aborted. The controller will be reset to its default state.' Below the message is a question: 'Are you sure you want to clear the selected controller's configuration?' At the bottom right are two buttons: 'Clear' (highlighted with a red border) and 'Cancel'.

A new window displays controller's settings and configuration.

5. To continue, click on **Finish**.

After clearing the Smart Array Controller:

1. Re-create the logical drives as described in the AW Server 3.2 Hardware Installation Manual, Re-creating Logical Drives.
2. Re-install the AW Server and restore the AW Server configuration as described in the AW Server 3.2 Installation and Service Manual, Job Card UPG001 - Software Upgrade.

3.17.4 Master Encryption Key in Local Key Management Mode

Local Key Management uses a Master Encryption Key (Master Key) to set the security on the controller and enable encryption. The Master Encryption Key must be tracked independently of the controllers in case the controller needs replacement or drive migration is required among controllers with different passwords.

Important

In local mode, the Master Encryption Key name is considered a cryptographic secret and should be protected as such. Key creation and management are maintained at local controller level without the use of a key manager.

The Master Encryption Key in Local Key Management Mode:

- Requires physical paraphrase password management, such as writing and storing Master Encryption Key information in a notebook or computer file.
- Utilizes one paraphrase password-derived 256-bit key to encrypt a unique, per-volume XTS-AES 256-bit data encryption key.

NOTICE

IMPORTANT PROCESS REQUIREMENT

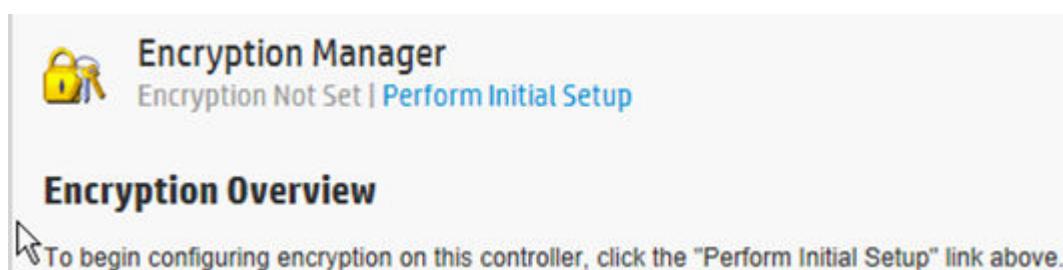
A record of the Master Encryption Key must be kept on customer site. The Master Encryption Key is not displayed by any available tool or firmware because it is considered as a cryptographic secret by FIPS 140-2. Secure Encryption design follows the NIST architecture requirements and does not allow for server manufacturer to assist in the recovery of a lost Master Encryption Key.

To configure Secure Encryption using command line or scripting methods, see the HPE Smart Storage Administrator User Guide.

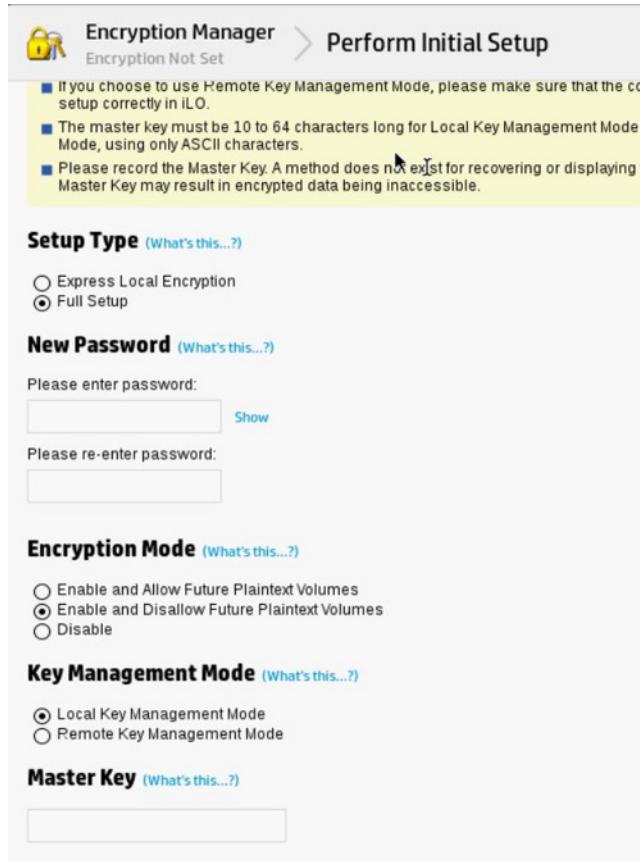
3.17.5 Configuring the Smart Array Controller for Local Key Management Mode

Prerequisites:

- An installed Smart Array Controller compatible with Secure Encryption
 - A valid Secure Encryption license for the server to be encrypted. This license must be purchased, but it does not need to be input into HPE Smart Storage Administrator (HPE SSA).
 - HPE Smart Storage Administrator (HPE SSA) v1.60.xx.0 and later
1. Open Encryption Manager.
See [3.17.1 Accessing Encryption Manager on page 371](#).
 2. Click on **Perform Initial Setup**.



The following screen appears:



3. Under **Setup Type**, select **Full Setup**.
4. In the **New Password** fields, enter and re-enter the Crypto Officer password in the fields provided.
5. Under **Encryption Mode**, select **Enable and Disallow Future Plaintext Volumes**. This option prevents the creation of new plaintext volumes on the controller. This setting can be changed later by the Crypto Officer. Selecting this option does not prevent the migration of a set of drives with existing plaintext volumes to the controller.
6. Under **Key Management Mode**, select **Local Key Management Mode**.
7. In the **Master Key** field, enter the Master Encryption Key.
 It must be between 10 and 64 characters.
8. Click on **OK**.
 A warning appears, prompting the user to record the Master Encryption Key.
9. Click **Yes** to continue.
10. If you have read and agree to the terms of the EULA, select the checkbox and click on **Accept**.
 A summary screen indicates the controller has been successfully configured for encryption use.
11. Click on **Finish** to continue.

The *Encryption Manager* screen appears with updated settings options.

Settings

| | | |
|--------------------------------|----------------------------|--|
| Encryption | Enabled | Disable Encryption |
| Key Management Mode | Remote Key Management Mode | Change |
| Master Key | Set | Change Master Key |
| Allow New Plaintext Volumes | Allow | Disallow Plaintext Volumes |
| Controller Password | Not Set | Set/Change Controller Password |
| Firmware Locked for Update | Unlocked | Lock Firmware |
| Controller Locked | Unlocked | |
| Local Key Cache Enabled | No | Set/Change Local Key Cache |
| Encrypted Physical Drive Count | 5 | Drive Key Rekey |

12. Under **Settings**, click on **Remove Controller Password**.

A window asks you to confirm that you want to remove the controller password.

13. Click on **Yes**.

3.17.6 Recovering the Crypto Officer Password

1. Open Encryption Manager.
See [3.17.1 Accessing Encryption Manager on page 371](#).
2. Under **Accounts**, click on **Recover Crypto Officer Password**.

Accounts

| | | |
|---|-----|---|
| Crypto Officer Password | Set | Set/Change Crypto Officer Password
Recover Crypto Officer Password |
| Crypto Officer Password Recovery Parameters | Set | Set/Change Password Recovery Question |
| User Password | Set | Set/Change User Password |

The following window appears:

Password Recovery Answer ([What's this...?](#))

Your question: motorbike I own and ride

New Password ([What's this...?](#))

Please enter password:

Please re-enter password:

3. In the **Password Recovery Answer** field, answer the security question.
4. In the **New Password** fields, enter and then re-enter a new password.
5. Click on **OK**.

3.17.7 Lost or forgotten Master Encryption Key

Important

Important Process Requirement

A record of the Master Encryption Key must be kept on customer site. The Master Encryption Key is not displayed by any available tool or firmware because it is considered as a cryptographic secret by FIPS 140-2. Secure Encryption design follows the NIST architecture requirements and does not allow for server manufacturer to assist in the recovery of a lost Master Encryption Key.

In Local Key Management Mode, securing the Master Encryption Key value is critical to accessing the encrypted logical drive data. If the controller requires replacement or if the physical drives are moved to another controller, a matching Master Key is required to gain access to the data. Master Encryption Keys are not recoverable if lost. If the Master Encryption Key is lost or forgotten, you must perform a data restore operation from the backup media to regain access to the data.

3.17.8 Replacing an Encrypted Smart Array Controller

If some or all the drives managed by the controller being replaced are encrypted, you must re-configure the replacement controller with the same settings and key management mode you used for the controller you are replacing. For more information, see the documentation that ships with the controller.

Secure Encryption is supported on HPE Smart Array PX3X and PX4X controllers, and on HX4X HPE Smart HBAs operating in RAID mode.

In Local Key Management Mode, you must provide the correct Master Encryption Key name that matches the one used for the attached drives.

3.17.9 Changing the password recovery settings

1. Open Encryption Manager.
See [3.17.1 Accessing Encryption Manager on page 371](#).
2. Under Accounts, click on **Set/Change Password Recovery Question**.

| Accounts | | |
|---|-----|---|
| Crypto Officer Password | Set | Set/Change Crypto Officer Password |
| Crypto Officer Password Recovery Parameters | Set | Set/Change Password Recovery Question |
| User Password | Set | Set/Change User Password |

The following window appears:

Password Recovery Question [\(What's this...?\)](#)

Password Recovery Answer [\(What's this...?\)](#)

3. In the **Password Recovery Question** field, enter a question to which only you know the answer.

4. In the **Password Recovery Answer** field, enter the answer to the question entered.
5. Click on **OK**.

3.18 Log patterns for log analysis in RMF environments

In RMF mode, AW Server sends various logs to the central log server which the customer can parse for further processing and log analysis. After processing the logs, reporting, and alerting can be done so that the designated personnel (such as the Information Management Officer [IMO], Information System Security Officer [ISSO] or the System Administrators [SAs]) within the DoD supervised organization gets notified about important statistics and events.

Note that in Generic mode, forwarding logs to the central log server is also possible but optional and there is a slightly different set of logs forwarded than discussed here.

3.18.1 Notifications when disk usage reaches a predefined level

Related STIG ID: RHEL-07-030350

The following log patterns can be parsed on the central log server:

```
'WARNING: <partition's name> partition fullness reached the first level(75%)... Please revise what logs can be deleted. Current usage is: <calculated disk usage>%'  
'ERROR: <partition's name> partition is almost full... Please revise what logs can be deleted. Current usage is: <calculated disk usage>%'  
'ERROR: <partition's name> partition is full... Please take immediate action to avoid unexpected behaviours!'  
'ERROR: Log partition is full, manual log clean up has been triggered to avoid data loss...'  
'INFO: Log cleanup finished. Log partition usage after cleanup: <calculated disk usage>.'
```

NOTE

If the **INFO** log about the finished cleanup does not arrive, then possibly a failure occurred during the cleanup process.

3.18.2 Notifications when an error sends audit records to a remote system

Related STIG ID: RHEL-07-030321

Log patterns:

```
'audisp-remote: GSS-API error reading token length'  
'audisp-remote: Error connecting to <log server's name>: Connection refused'  
'audisp-remote: network failure, max retry time exhausted'  
'audisp-remote: network failure, max retries exhausted'
```

3.18.3 AIDE logs

Related STIG IDs: APSC-DV-001370, RHEL-07-020030, RHEL-07-020040

AIDE logs are sent to the central log server in case of any integrity check fails on the files being monitored.

Log patterns:

```
'AIDE 0.15.1 found differences between database and filesystem!!  
Start timestamp: {year}-{month}-{day} {hour}:{minute}:{second}'
```

```

Summary:
Total number of files:      {number of files}
Added files:                {number of added files}
Removed files:              {number of removed files}
Changed files:              {number of changed files}

-----
Added files:
-----
added: {path of added file, eg. /home/test_conf.db }
added: {path of added file}

-----
Removed files:
-----
removed: {path of removed file}

-----
Changed files:
-----
changed: : {path of changed file eg. /home/test_conf.db.new.gz}

-----
Detailed information about changes:
-----
File: /home/test_conf.db.new.gz
Size : 0 ,                               1071
SHA256 : 47DEQpj8HBSa+/TImW+5JCeuQeRkm5NM , m0MEGwcMQkoqbMDCJB6YQNzdVump6XZ1 '

```

3.18.4 McAfee logs

STIG requirement ID: RHEL-07-020019

On the AW Server system the “on access scan detection events” are configured to be synchronized to the central log server. These logs are stored in the following log file on AW Server:

`/var/McAfee/ens/log/tp/mfescanactionmgr.log`

The log format is containing a date-time, hostname, log level, module, PID and an event description.

Example event log:

```
Apr 22 19:07:35 localhost INFO ScanActionMgr [3479] Scan Action Manager is startin g
```

The following table lists important event IDs that Endpoint Security for Linux Threat Prevention generates and which are sent to the central log server (OAS event types):

| Event ID | Description (Severity) |
|----------|---|
| 1024 | Infected file found, access denied (High) |
| 1025 | Malware cleaned (Info) |
| 1026 | Malware clean failed (Info) |
| 1027 | Malware deleted (Info) |
| 1028 | Malware delete failed (Info) |
| 1046 | File I/O errors (Info) |
| 1048 | Scan reports general system error (Info) |
| 1051 | Unable to scan, password protected (Medium) |
| 1053 | Infected file found (High) |
| 1059 | Scan timed out (Medium) |
| 1087 | On-access scan started (Info) |
| 1088 | On-access scan stopped (Info) |
| 1100 | Macro detected in file (Low) |

| Event ID | Description (Severity) |
|----------|--|
| 1278 | File infected. No cleaner available, file deleted successfully. (Info) |
| 1282 | File infected. No cleaner available, delete failed. (High) |
| 1289 | File infected. Clean error, encrypted file, continued scanning. (High) |
| 1290 | File infected. No cleaner available, denied access and continued. (High) |
| 1291 | File infected. Clean error, heuristic detection, denied access and continued. (High) |
| 1300 | File infected. Delete failed, denied access and continued. (High) |

On the AW Server the McAfee component fully controls its local log management. See details here:

<https://docs.trellix.com/bundle/endpoint-security-10.7.0-threat-prevention-product-guide-linux/page/GUID-79CFC24E-C305-46C8-BE9A-338D8A597F20.html>

3.18.5 Hardware failures

Related STIG ID: APSC-DV-001110

Standard logs of Hewlett Packard Enterprise Integrated Lights-Out (HPE ILO) are used.

Examples from ILO ver. 4:

Drive array:

```
'Internal Storage Enclosure Device Failure (Bay 8, Box 1, Port 2I, Slot 0)'
```

Environment:

```
'System Overheating (Temperature Sensor 1, Location Ambient, Temperature 42C)'
```

Maintenance:

```
'IML Cleared (iLO 4 user:root)'
```

OS:

```
'Automatic Operating System Shutdown Initiated Due to Overheat Condition'
```

POST message:

```
'POST Error: 1720-Slot X Drive Array - S.M.A.R.T. Hard Drive(s) Detect imminent failure'
```

Power:

```
'System Power Supply: Input Power Loss or Unplugged Power Cord, Verify Power Supply Input Power Supply 2)'
```

System Revision:

```
'Firmware flashed (iLO 4 2.70)'
```

Related documents:

https://support.hpe.com/hpsc/public/docDisplay?docId=emr_na-c01742395#N10011

https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c01702138

https://support.hpe.com/hpsc/public/docDisplay?docId=c03255140&docLocale=en_US

3.18.6 Apache web server logs

Related STIGs: AS24-U1-000065, AS24-U1-000070

Standard Apache logs are used in AW Server.

Example for restart:

```
'AH00171: Graceful restart requested, doing restart'
```

Example for shutdown:

```
'AH00170: caught SIGWINCH, shutting down gracefully'
```

Related documents:

<https://cwiki.apache.org/confluence/display/httpd/ListOfErrors>

<https://httpd.apache.org/docs/2.4/logs.html>

3.18.7 EAT logs

Related STIG IDs: APSC-DV-001080, APSC-DV-001070

EAT generated Audit Event messages are compliant with RFC 3881 extended by DICOM schema (Defined in DICOM part 15) and by IHE IT Infrastructure Domain Audit Trail and Node Authentication (ATNA) Profile.

Following clinical/application events are audit logged through EAT:

- User login (Success/Failure)
- User creation
- User deletion
- User password change
- Group assignment of users
- Access and modification to patient data
- Patient deletion
- DICOM study/series deletion
- DICOM query from a remote host
- DICOM query to a remote host
- DICOM push from a remote host
- DICOM pull from a remote host
- Preference import
- Preference snapshot creation
- Firewall settings
- App launch / close
- DICOM Data import
- Data export

Examples:

Database access

```
<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage>
    <EventIdentification EventActionCode="E" EventDateTime="2022-04-29T10:50:01" EventOutcomeIndicator="0">
        <EventID csd-code="110113" codeSystemName="DCM" originalText="Security Alert"/>
        <EventTypeCode csd-code="110137" codeSystemName="DCM" originalText="User s
```

```

    security Attributes Changed"/>
  </EventIdentification>
  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="true" NetworkAccessPointTypeCode="1"
    NetworkAccessPointID="{ NetworkAccessPointID }"></ActiveParticipant>
  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="false"></ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="">
    <AuditSourceTypeCode csd-code="9" codeSystemName="DCM" originalText="External source, other or unknown type"/>
  </AuditSourceIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="{ ParticipantObjectID }"
    ParticipantObjectTypeCode="2" ParticipantObjectTypeCodeRole="13">
    <ParticipantObjectIDTypeCode csd-code="12" codeSystemName="RFC-3881" originalText="">
      <ParticipantObjectName/>
      <ParticipantObjectDetail type="Alert Description" value="VXNlciBwYXNzd29yZCBjaGFuZ2VkLg=="/>
    </ParticipantObjectIdentification>
  </AuditMessage>

```

System access

```

<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage>
  <EventIdentification EventActionCode="E" EventDateTime="2022-04-29T10:50:08" EventOutcomeIndicator="0">
    <EventID csd-code="110114" codeSystemName="DCM" originalText="User Authentication"/>
    <EventTypeCode csd-code="110122" codeSystemName="DCM" originalText="Login"/>
  </EventIdentification>
  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="true" NetworkAccessPointTypeCode="1" NetworkAccessPointID="devaws-brn.aw.health.ge.com">
    <RoleIDCode csd-code="110150" codeSystemName="DCM" originalText="Application"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="false" NetworkAccessPointTypeCode="1" NetworkAccessPointID="{ NetworkAccessPointID }"></ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="">
    <AuditSourceTypeCode csd-code="9" codeSystemName="DCM" originalText="External source, other or unknown type"/>
  </AuditSourceIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="Detail">
    <ParticipantObjectIDTypeCode csd-code="" codeSystemName="" originalText="">
  </ParticipantObjectIdentification>
</AuditMessage>

```

Opening Application - DICOM access

```

<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage>
  <EventIdentification EventActionCode="R" EventDateTime="2022-04-29T10:55:41" EventOutcomeIndicator="0">
    <EventID csd-code="110103" codeSystemName="DCM" originalText="DICOM Instances Accessed"/>
  </EventIdentification>
  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="false"></ActiveParticipant>

```

```

  <ActiveParticipant UserID="{ UserID }" UserIsRequestor="true"></ActiveParticipant>
    <AuditSourceIdentification AuditSourceID="">
      <AuditSourceTypeCode csd-code="9" codeSystemName="DCM" originalText="External source, other or unknown type"/>
    </AuditSourceIdentification>
    <ParticipantObjectIdentification ParticipantObjectID="patientID" ParticipantObjectTypeCode="1"
      ParticipantObjectTypeCodeRole="1">
      <ParticipantObjectIDTypeCode csd-code="2" codeSystemName="RFC-3881" originalText="Patient Number"/>
      <ParticipantObjectName/>
    </ParticipantObjectIdentification>
    <ParticipantObjectIdentification ParticipantObjectID="{ParticipantObjectID}"
      ParticipantObjectTypeCode="2" ParticipantObjectTypeCodeRole="3">
      <ParticipantObjectIDTypeCode csd-code="110180" codeSystemName="DCM" originalText="Study Instance UID"/>
      <ParticipantObjectName/>
    </ParticipantObjectIdentification>
    <ParticipantObjectIdentification ParticipantObjectID="Detail">
      <ParticipantObjectIDTypeCode csd-code="" codeSystemName="" originalText="" />
      <ParticipantObjectName/>
      <ParticipantObjectDetail type="Detail" value="PGxpY2Vuc2VOYW1lPlZvbHvtZV9WaWV3ZXI8L2xpY2Vuc2VOYW1lPg=="/>
    </ParticipantObjectIdentification>
  </AuditMessage>

```

Related documents:

RFC 3881: <https://www.ietf.org/rfc/rfc3881.txt> (XML Schema definition at section 6.1)

DICOM Standard Part 15: <http://dicom.nema.org/standard.html>

IHE IT ATNA Profile: https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

3.18.8 Audit logs for monitored syscalls

Related STIG IDs: RHEL-07-030880, RHEL-07-030890, RHEL-07-030900, RHEL-07-030910, RHEL-07-030910, RHEL-07-030920 etc.

Syscalls: create, truncate, ftruncate, rename, renameat, unlink, unlinkat, delete_module, create_module, finit_module, init_module, chown, fchown, lchown, fchownat, chmod, fchmod, fchmodat, setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, lremovexattr

Syscalls monitored only for RMF mode: open, openat, open_by_handle_at

Example:

```

'Feb 28 22:01:27 vht224f audispd: node=vht224f type=SYSCALL
msg=audit(1646082087.760:17538): arch=c000003e syscall=268 success=yes exit=0
a0=fffffffffffff9c a1=20750f0 a2=120 a3=7ffd6dfffd360 items=1 ppid=26800 pid=2688
6
auid=0 uid=0 gid=0 euid=0 suid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=518
comm="chmod" exe="/usr/bin/chmod" key="privileged-actions"

```

Related document:

Red Hat Enterprise Linux 7 Security Guide section 7.6. Understanding

Audit Log Files https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files

3.18.9 Audit logs for monitored commands

Related STIG IDs: RHEL-07-030630, RHEL-07-030650, RHEL-07-030660, RHEL-07-030670, RHEL-07-030710, RHEL-07-030720 etc.

Commands: rmdir, crontab, mount, umount, pam_timestamp_check, passwd, gpasswd, chage, userhelper, postdrop, postqueue, ssh-keysign, semanage, setsebool, chcon, setfiles, chsh, newgrp

Commands monitored only for RMF mode: su, sudo, /sbin/insmod, /sbin/unix_chkpwd

Example:

```
'Mar 26 18:55:31 vlt150f audispd: node=vlt150f type=SYSCALL
msg=audit(1648317331.262:117121): arch=c000003e syscall=2 success=yes exit=4
a0=7fd47b2c132e a1=2 a2=457 a3=3 items=1 ppid=27464 pid=27465 auid=4294967295 uid=
0
gid=0 euid=0 suid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="
su"
exe="/usr/bin/su" key="logins"'
```

Related document:

Red Hat Enterprise Linux 7 Security Guide section 7.6. Understanding

Audit Log Files https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files

3.18.10 GEHC concept template

Related STIG IDs: RHEL-07-030870, RHEL-07-030871, RHEL-07-030872, RHEL-07-030873, RHEL-07-030874 etc.

Files (identity): /etc/passwd, /etc/group, /etc/gshadow, /etc/shadow, /etc/security/opasswd

Files (logins): /var/run/faillock, /var/log/lastlog

Monitored only for RMF: /etc/sudoers, /etc/sudoers.d/

Example:

```
'Mar 24 08:40:40 vlt141f audispd: node=vlt141f type=PATH
msg=audit(1648107640.982:75078): item=0 name="/var/log/lastlog" inode=15 dev=08:0
2
mode=0100644 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000
cap_fi=0000000000000000 cap_fe=0 cap_fver=0'
```

Related document:

Red Hat Enterprise Linux 7 Security Guide section 7.6. Understanding

Audit Log Files https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files

3.18.11 General notes on logs in RMF mode

AW Server service processes are generally using the operating system's logging mechanism to log application (user level) generated logs into the local filesystem and synchronize it with a remote logging server if remote logging is enabled.

Kernel logging

Related STIG ID: RHEL-07-030010

Kernel log monitoring is enabled on AWS in RMF mode, and the following log levels have been defined (standard linux kernel log levels):

Level	Description
KERN_EMERG	It is adopted by messages about system instability or imminent crashes.
KERN_ALERT	This level is used in situations where the user attention is immediately required.
KERN_CRIT	This level of severity is used to inform about critical errors, both hardware or software related.
KERN_ERR	Messages adopting this level are often used to notify the user about non-critical errors, as for example a failed or problematic device recognition, or more generally driver-related problems.
KERN_WARNING	This level is used to display warnings or messages about non imminent errors.
KERN_NOTICE	Messages which use this level of severity are about events which may be worth noting.
KERN_INFO	This is the log level used for informational messages about the action performed by the kernel.
KERN_DEBUG	Mainly used for debugging.

Low-level services

For low-level (OS based) applications, the syslog protocol's log levels are applicable:

Value	Severity	Keyword
0	Emergency	emerg
1	Alert	alert
2	Critical	crit
3	Error	err
4	Warning	warning
5	Notice	notice
6	Informational	info
7	Debug	debug

High-level (Java based) services

For high level applications, AWS is mainly using log4j as a logging provider, so the log4j logging levels are applicable:

Level	Description
ALL	All levels including custom levels.
DEBUG	Designates fine-grained informational events that are most useful to debug an application.
INFO	Designates informational messages that highlight the progress of the application at coarse-grained level.
WARN	Designates potentially harmful situations.
ERROR	Designates error events that might still allow the application to continue running.
FATAL/SEVERE	Designates very severe error events that will presumably lead the application to abort.
OFF	The highest possible rank and is intended to turn off logging.
TRACE	Designates finer-grained informational events than the DEBUG.

General logging configurations

Related STIG ID: RHEL-07-031000, APSC-DV-001080

In below table you can find the rsyslog configurations for the services, and the corresponding log files:

RSYSLOG CONF	LOG(S)
21-cloudinit.conf	/var/log/cloud-init.log
application-svc.conf	/var/log/gehc/application-svc/application-svc.log
applist-svc.conf	/var/log/gehc/applist-svc/applist-svc.log
auth-service.conf	/var/log/gehc/auth-service/auth-service.log
awsmonitor.conf	/var/log/gehc/awsmonitor/awsmonitor.log
awsmon-processer.conf	/var/log/gehc/awsmon-processer/awsmon-processer.log
awsservicermi.conf	/var/log/gehc/awsservicermi/awsservicermi.log
aws-watchdog.conf	/var/log/gehc/aws-watchdog/aws-watchdog.log /var/log/gehc/ServiceTools/log/watchdog/watchdog.log
cola-server.conf	/var/log/gehc/cola-server/cola-server.log
component-registration-rsyslog.conf	/var/log/gehc/component-registration/component-registration.log
configuration-service.conf	/var/log/gehc/configuration-service/configuration-service.log
csi-echoservice.conf	/var/log/gehc/csi-echoservice/csi-echoservice.log
csi-neta.conf	/var/log/gehc/csi-neta/csi-neta.log
dicomdir-svc.conf	/var/log/gehc/dicomdir-svc/dicomdir-svc.log
ea3-rsyslog.conf	/usr/share/gehc_security/ea3/logs/ea3SrvOut
els-server.conf	/var/log/gehc/els/els-service.log
endofreview-svc.conf	/var/log/gehc/endofreview-svc/endofreview-svc.log
filetransfer-server.conf	/var/log/gehc/filetransfer-server/filetransfer-server.log
listen.conf	/run/systemd/journal/syslog
mailsender-service.conf	/var/log/gehc/mailsender-service-mailsender-service.log
mediacreator-app.conf	/var/log/gehc/mediacreator-app/mediacreator-app.log
pacsinteg-webservice.conf	/var/log/gehc/pacsinteg-webservice/pacsinteg-webservice.log
rmp-server.conf	/var/log/gehc/rmp-server/rmp-server.log
servicermi.conf	/var/log/gehc/servicermi/servicermi.log
visualization-svc.conf	/var/log/gehc/visualization-svc/visualization-svc.log
dod_log_forward.conf	/var/log/dod_install.log
aide_log_forward.conf	/var/log/aide/aide.log
mcafee_log_forward.conf	/var/McAfee/ens/log/tp/mfescanactionmgr.log

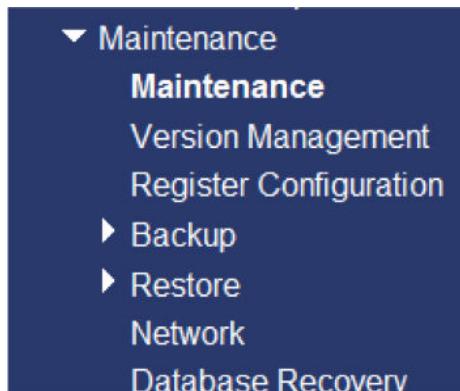
Chapter 4 AW Server Platform Maintenance

4.1 Overview

This chapter explains procedures associated with the tools provided under the **Maintenance** category of the AW Server's Service Tools.

- [Section 4.2 Maintenance Mode on page 388](#)
- [Section 4.3 Client Broadcast Message on page 392](#)
- [Section 4.4 Configuration Backup on page 394](#)
- [Section 4.5 Configuration Restore on page 401](#)
- [Section 4.6 Version Management on page 406](#)
- [Section 4.7 Network Reconfiguration on page 409](#)
- [Section 4.8 Database Recovery on page 414](#)
- [Section 4.9 Register Configuration on page 416](#)

4.2 Maintenance Mode



NOTE

Maintenance is a Service Tools menu heading, which also includes (among others) a **Maintenance** tool in one of its sub-menus.

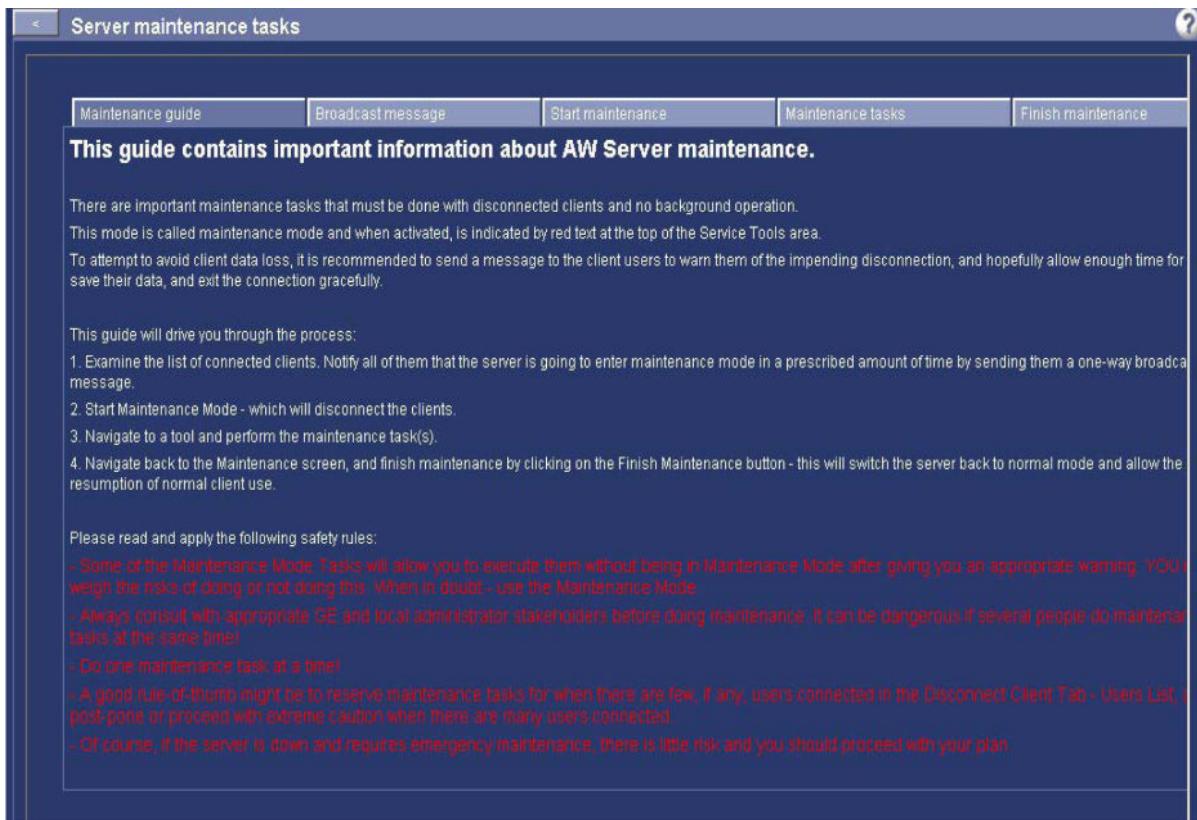
The menu choices under the Maintenance heading are described as follows:

4.2.1 Understanding the Maintenance Mode

There are important server maintenance tasks that must be done only when all clients have been disconnected and when no background operations are in progress. Maintenance mode is a process that can safely perform these functions without unexpectedly disconnecting clients or corrupting user files. It is indicated by a red text at the top of the Service Tools area.

NOTE

Maintenance mode is a combination of a tool and a process, and needs to be used within the context of the needed service intervention. It is NOT a “one-size-fits-all” or “one-button-and-done” tool.

Figure 4-1 MAINTENANCE MODE GUIDE PAGE

In the Service Tools web interface, click on **Maintenance**. The entry / home screen for the Maintenance Mode Page is the **Maintenance Guide Tab**.

The correct process to use Maintenance Mode is the following:

1. Examine the list of connected clients, using the **Start Maintenance** tab.
2. Notify all of them that the server is going to enter maintenance mode in a prescribed amount of time by sending them a one-way **broadcast message** (using the **Broadcast message** tab). Allow enough time for them to save their data, for example 5-10 minutes.
3. Start Maintenance Mode, using the **Start maintenance** tab.
4. When done with your maintenance tasks, finish the Maintenance Mode, using the **Finish Maintenance** tab.

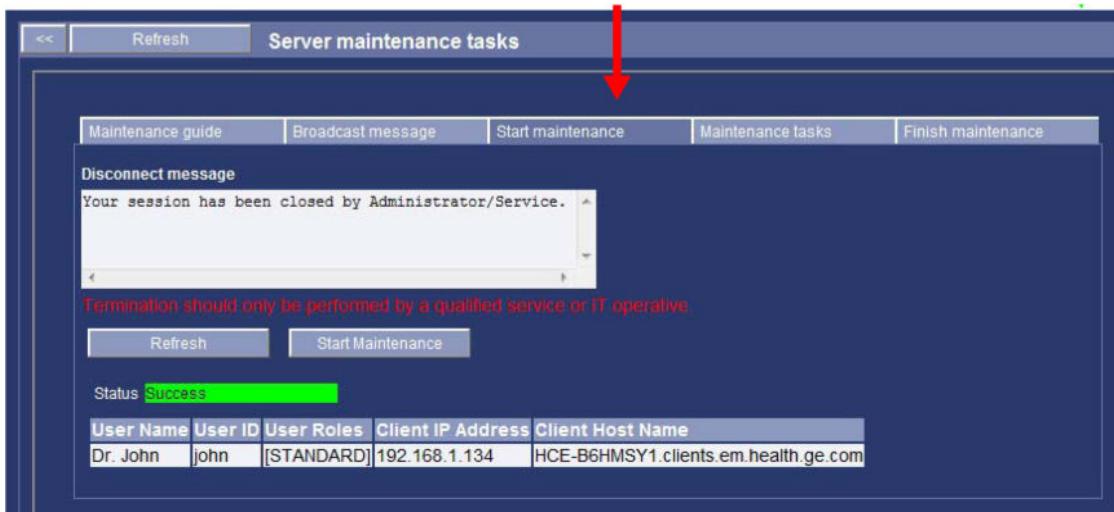
The next sections provide details for each of these steps.

NOTICE

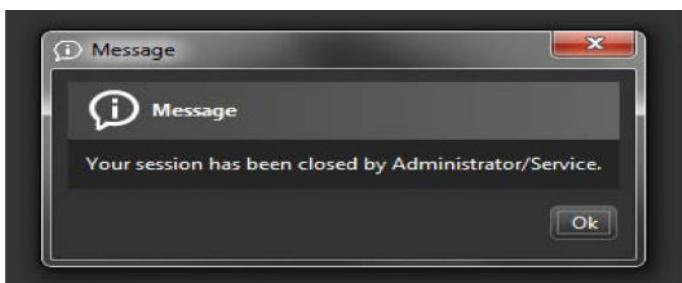
In the case of a cluster of AW Servers, you must log on to all AW Servers in a cluster to broadcast the message. There is no central location to activate this task.

4.2.2 Start Maintenance Mode

Navigate to the **Maintenance > Maintenance** menu in Service Tools. Click on the **Start Maintenance** tab. Enter a message to warn the users, then click on **Start Maintenance**. This will disconnect the clients.



On the AWS Client side, the users will be disconnected and see a warning message:



You can now perform the maintenance task(s).

NOTICE

**WHEN THE SYSTEM IS IN MAINTENANCE MODE, CLIENTS CANNOT LOGIN.
IT IS IMPORTANT NOT TO LEAVE THE SYSTEM IN MAINTENANCE MODE
ACCIDENTALLY...**

Please read and apply the following rules:

- Some of the Maintenance Mode Tasks will allow you to execute them without being in Maintenance Mode after giving you an appropriate warning. **YOU must weigh the risks of doing or not doing this. When in doubt – use the Maintenance Mode.**
- **Always consult with appropriate GE and local admin stake-holders before doing maintenance.** The system might crash if several people do maintenance tasks at the same time!
- Do one maintenance task at-a-time!
- A good rule-of-thumb might be to reserve maintenance tasks for when there are **few if any users connected** in the Disconnect Client Tab – Users List, and to postpone or proceed with caution when there are many users connected.
- Of course, if the server is down there are no clients connected anyway, there is little risk, and you should proceed with your plan immediately.

Be aware that the Broadcast messaging tool is a **ONE-WAY** communication. You will not receive, or should you expect any acknowledgment of messages sent using this tool. **If you have concerns regarding a particular user or users, please stray on the side of caution and make direct contact with them to be certain of your plans before you execute them.**

Always be sure to check what is in the message box before you send (**to make sure the correct message is sent**), and when you finish (**to make sure the old message is extinguished and not sent again for no reason**).

- After reading and understanding the guide tab, begin your Maintenance Mode process, click on the **Broadcast Message Tab** (see [4.3 Client Broadcast Message on page 392](#)), and proceed through the steps.

NOTICE

Once started, the AW Server stays in Maintenance Mode, even after a reboot. The only way to finish Maintenance is to use the correct Service Tools menu Maintenance > Maintenance > Finish Maintenance.

NOTE

The Universal Viewer can be blocked when the Maintenance is activated and the end user has not acknowledged the broadcast message. In this case, the user will have to exit from the Universal Viewer by using the Tasks Manager or by rebooting the PC.

4.2.3 Maintenance Mode Banner

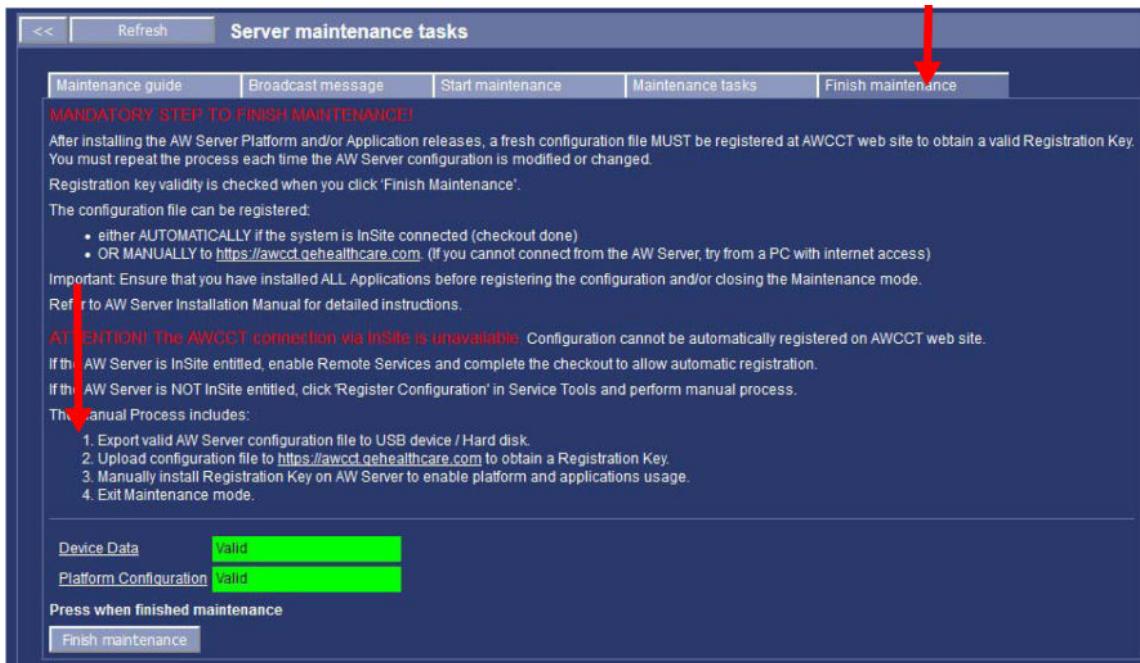
When the AW Server is in Maintenance Mode, a banner is displayed at the top of the Service Tools as follows:



This banner is displayed on all Service Tools pages and provides a simple way to know if the AW Server is in Maintenance Mode. It also provides the number of Service Tools tasks currently running on the AW Server.

4.2.4 Finish Maintenance Mode

When maintenance tasks are completed, to exit from the Maintenance mode, click on the **Finish maintenance** tab, then on the **Finish maintenance** radio button. This will switch the server back to normal mode and allow the resumption of normal client use.



NOTICE

Before finishing maintenance mode, it is mandatory to do all the following:

- Fill in all mandatory fields in Device Data
- Obtain a registration key
- Apply the Platform Configuration (platform key, cluster mode, integration settings)

If one of the above conditions is not fulfilled, it will not be possible to finish maintenance mode.

The number of the running maintenance tasks is indicated. End of Maintenance can be forced if necessary.

In some cases, if any maintenance tasks remain, a message will be displayed to ask confirmation that Maintenance shall be finished beside this. *Do you really want to finish? Number of running maintenance mode tasks: X*

NOTICE

Forcing end of maintenance may leave the system in an inconsistent state. Software Subsystem restart on HealthPage or reboot is a must. Load-From-Cold might be also needed.

NOTICE

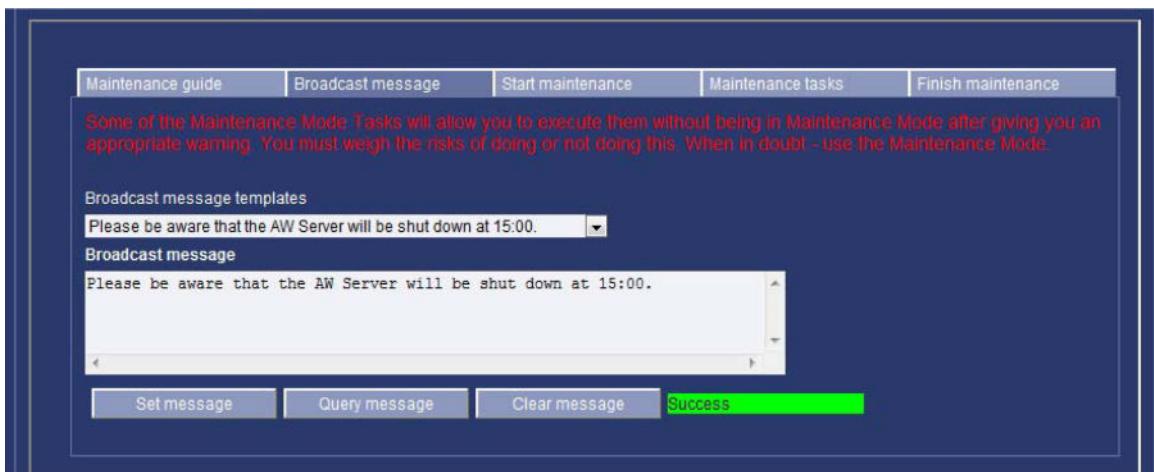
Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

4.3 Client Broadcast Message

NOTE

This dialog is already covered in more details in [Chapter 2, 2.4.2 Utilities on page 78](#), as it is also accessible for the Administrator from the *Administrative > Utilities > Clients* menu.

4.3.1 Broadcast message



Broadcast message tool – This tool allows the capability to send a broadcast message to **ALL** connected clients of the selected AW Server. When there are multiple AW Servers, the broadcast message must be sent on each AW Server.

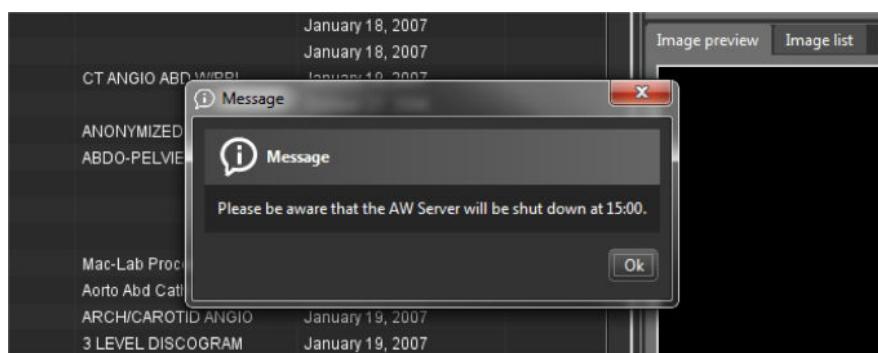
There are THREE control buttons for the message text.

Set message – this button sends whatever text is in the message box.

Query message – This button will display the current message text that is set-up to send.

Clear message – This button will clear the message text field. It is very important to remember to CLEAR your message texts after sending them – if you do not want the same message sent again unintentionally.

Figure 4-2 EXAMPLE MESSAGES APPEARING AT THE CLIENT BROWSER

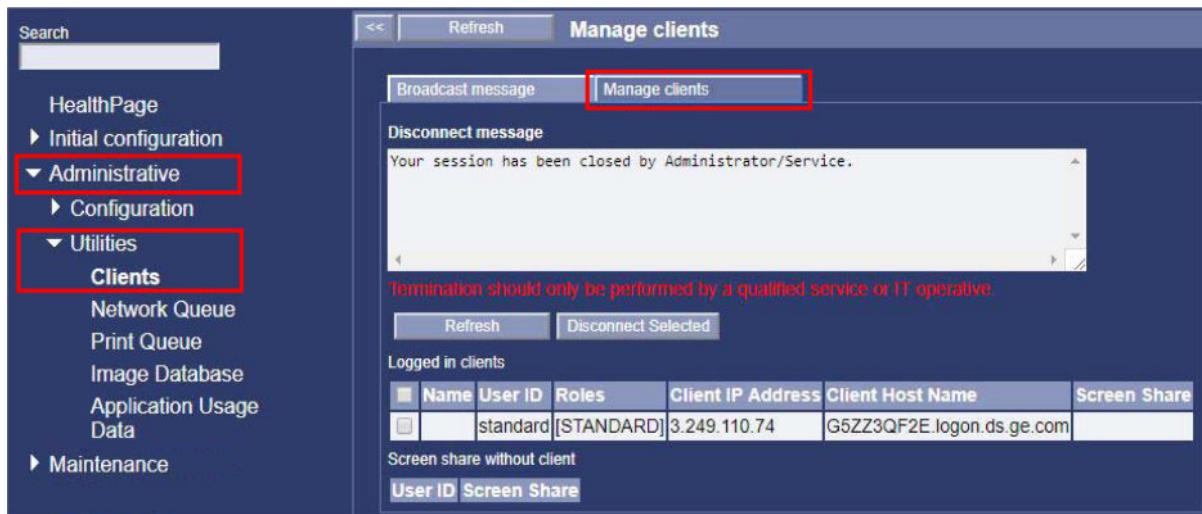


NOTE

The Universal Viewer can be blocked when the Maintenance is activated and the end user has not acknowledged the broadcast message. In this case, the user will have to exit from the Universal Viewer by using the Tasks Manager or by rebooting the PC.

4.3.2 Manage Clients

This tool is also accessible to the IT administrator of the site.



Manage Clients

This tool lists the Clients currently connected to the AWServer.

Refresh

Use this button often! There may be a certain amount of latency in the real-time ability of the tool to list current clients. The **Refresh** button may at time take a moment to update ...

Disconnect Selected

This button will disconnect listed clients if they are selected in the check box at the left of the list.

4.4 Configuration Backup

This menu sub-heading includes two backup tools as follows:

System configuration– This tool creates system configuration backup files. It shows a checklist of items that can be saved in the backup file. Items that have a arrow (▶) on their left side can be expanded to show the separate, specific sub-items within that category, which you can select or deselect as needed. Click the “Pull from system” button to transfer the backup file to the computer you’re using, or click “Save on system” to save the file on the AW Server.

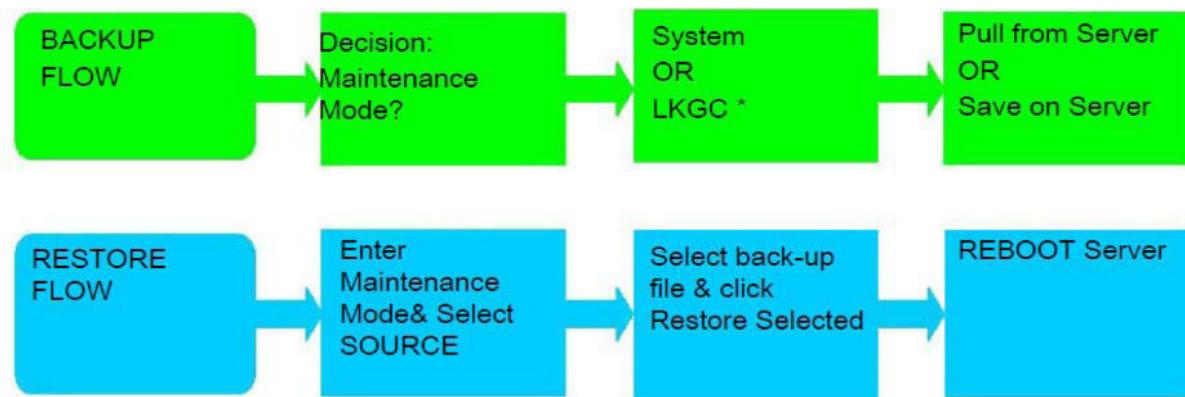
Comments

Any text entered in the Comments box will be saved with the backup file.

Recurrence

The Recurrence function lets you set a time for the system to automatically create these backup files, either daily, weekly, or monthly.

User preferences– This creates a backup file for user preferences. Use the list of users to select which users’ preferences will be backed up. Text entered into the “Comments” box is saved with the user preferences backup file. Click the “Pull from system” button to transfer the backup file to the computer you’re using, or click “Save on system” to save the file on the AW Server.

Figure 4-3 BACK-UP & RESTORE FLOW OVERVIEW

* **LKGC**= Last Known Good Configuration

Back Up of the system configuration files and user preference files is done through this tool in the Maintenance Menu tree.

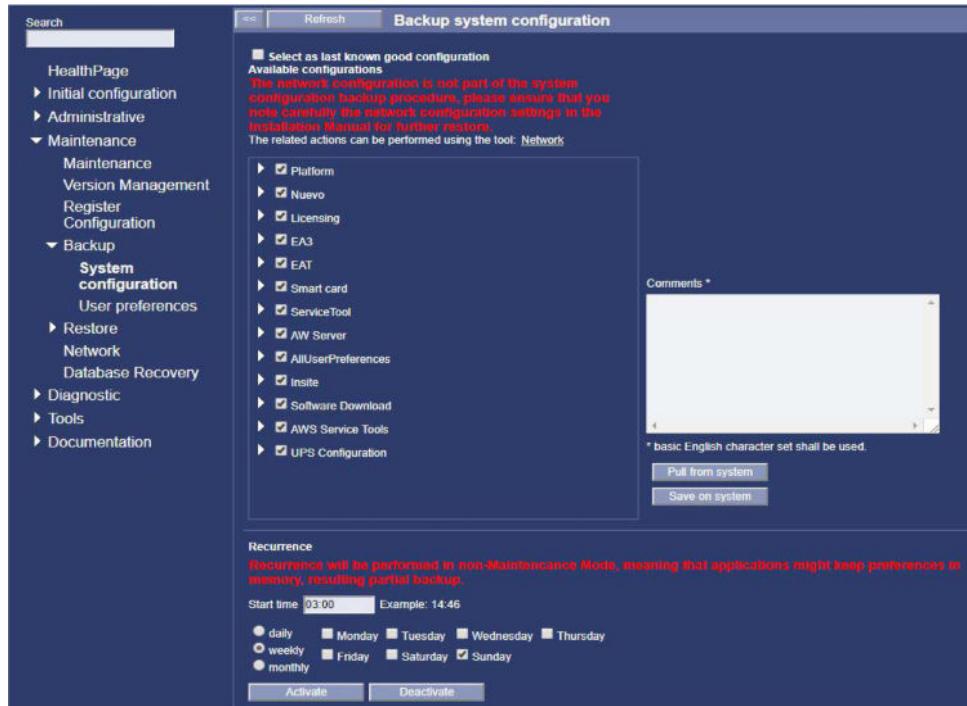
NOTE

Earlier in this chapter the Maintenance Mode was presented. This is one of the server maintenance activities recommended to be done within the **Maintenance Mode - to ensure corruption-free configuration files**.

However, it also one of those Maintenance Mode Tasks that has been designed to also allow **override** – or the ability to perform without initiating the Maintenance Mode – if it is deemed necessary.

NOTES about the BACKUP Utility:

- It is advisable to save or Back-Up system configuration as often as possible. Be aware if the system is under heavy use with multiple clients using it. Perform Back-Ups outside of Maintenance Mode only if you are sure the system is not being used – meaning the RISK of file corruption is low.
- For AW Server which are not in seamless or full integration, the AWServer Backup is saved in a specific partition. If there is a problem with the back-up process, check the HealthPage - Server Configuration - pane to make sure that Backup Partition Space is not full. It is not likely that this should ever happen due to the backup files size versus the available partition space, but it is a good place to start.
- For AW Server in seamless or full integration, identify a safe location with the IT Admin to save the Backup configuration.

Figure 4-4 CONFIGURATION BACK UP

4.4.1 System Configuration Backup

NOTE

System configuration backup also includes the backup of User Preferences (see [4.4.2 User Preferences Backup on page 399](#)).

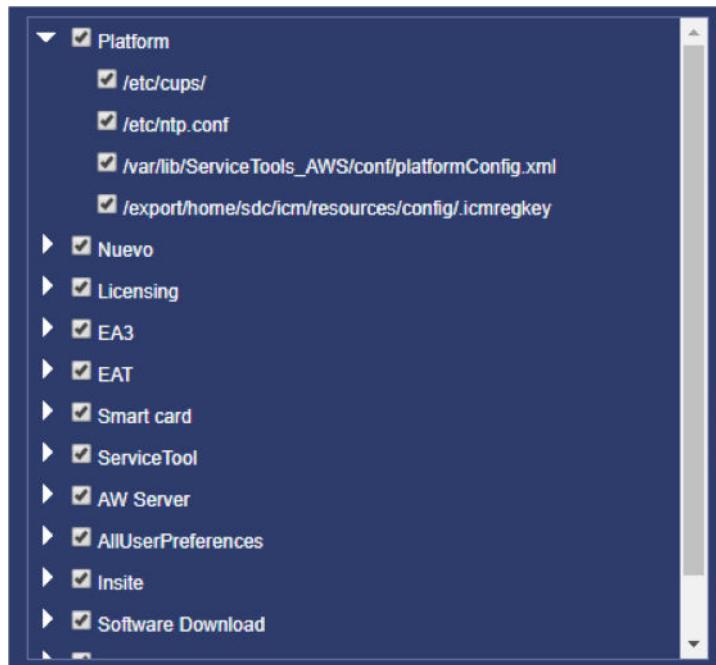
This is the “home” or default tab that is displayed when the Back-Up tool is accessed. There are a number of options available for selection or use on this page.

- **Select as last known good configuration** – If you select this box, the configuration files will automatically include **ALL** available configurations in the back up, and will effectively remove the option to individually select configurations in the list below the check box.

The last known good configuration (**LKGC**) is no different than a normal system back up, except for the following specific differences:

- **It is designed to always be a complete or total system back up.**
- It is saved in its own specific file system location, separate from the normal system back up file - /export/backup/last_known_good/AWBULAB_backupSyst_20140904-104734.tar.gz (this is an “example” file name to illustrate the naming convention)
- **It is meant to be a FULL system back up that can be used for system restoration to the last known good configuration after a service or failure scenario that has corrupted or deleted the current configuration.**
- As a point of recommendation, it is a good practice to back up the LKGC whenever you also back up system configuration for any other purpose.
- If the **LKGC** box is not checked, the “**Available configurations**” check box list will become active. This means that you can choose to save or back up **ALL** the system configuration files (like the LKGC), **or whatever sub-set of the system configuration files or file you choose**. The resultant back up file for this back up option is also a separate individual file, saved in a separate file-system location - /export/backup/system/AWBULAB_backupSyst_20140905-153842.tar.gz (this is an “example” file name to illustrate the naming convention)

- If you click on each available configuration **ARROW**, it will expand the selection, and display the **directory path** to the individual file(s) that are backed up when that selection is checked – as shown in the example below:



You will notice that the individual files are not always listed – just the directory paths. This is because there are many, many files involved in most cases, some of which may exist on a particular server configuration, some of which may not – some of which may contain data, some of which may not. Following are 3 screen-shots of a listing of the files that are contained in the saved back up archive file **for reference only**.

Use this as a general map to understand what file or files are saved in each general directory path if you are interested in knowing. If you are viewing this in electronic format, it might be easier to view it if you increase your viewing aspect ratio – magnify the text...

Figure 4-5 CONFIGURATION BACK UP FILES EXAMPLE (EXTRACT)

resources/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/terra/
dmf/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/terra/resources/dmf/
shortreliability.test	9,308	9,308	TEST File	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
DMFDicomCIOD.cfg	11,054	11,054	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
DMFDicomDict.cfg	61,532	61,532	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
DMFDicomModules.cfg	34,956	34,956	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
copy.test	366	366	TEST File	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
dmferror.cfg	12,413	12,413	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
lb.cfg	2,438	2,438	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
overandover.test	360	360	TEST File	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
reliability.test	15,466	15,466	TEST File	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/dmf/
terra.cfg	2,748	2,748	Microsoft Office Outlo	07/18/2008 11:49 AM	0.0% /export/home/sdc/terra/resources/
stream.cfg	268	268	Microsoft Office Outlo	06/27/2008 02:13 PM	0.0% /export/home/sdc/terra/resources/
resources/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/
archive/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/
JavaErrCodes.cfg	3,128	3,128	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/archive/
devConfig.cfg	787	787	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/archive/
errConfig.cfg	1,030	1,030	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/archive/
browser/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/
Applications.xml	2,506	2,506	XML Document	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/browser/
filters.xml	51	51	XML Document	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/browser/
sessions.properties	202	202	PROPERTIES File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/browser/
dbx/	0	0	File Folder	07/18/2008 11:52 AM	0.0% /export/home/sdc/nuevo/resources/
config/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/dbx/
postgresql.conf	11,028	11,028	CONF File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/config/
dmf/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/dbx/
shortreliability.test	9,308	9,308	TEST File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
DMFDicomCIOD.cfg	11,054	11,054	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
DMFDicomDict.cfg	61,532	61,532	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
DMFDicomModules.cfg	34,956	34,956	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
copy.test	366	366	TEST File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
lb.cfg	2,438	2,438	Microsoft Office Outlo	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
overandover.test	360	360	TEST File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
reliability.test	15,466	15,466	TEST File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/dmf/
procedures/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/dbx/
procedures-MR.sql	18,127	18,127	SQL File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/procedures/
procedures.sql	25,242	25,242	SQL File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/procedures/
schema/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/dbx/
schema_MR.sql	10,018	10,018	SQL File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/schema/
schema.sql	15,408	15,408	SQL File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/dbx/schema/
terra.cfg	2,748	2,748	Microsoft Office Outlo	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/dbx/
pg_xlog/	0	0	File Folder	07/18/2008 12:25 PM	0.0% /export/home/sdc/nuevo/resources/dbx/
archive_status/	0	0	File Folder	07/18/2008 11:52 AM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
0000000100000000000000000007	16,777,21	16,777,216	File	07/18/2008 12:13 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
0000000100000000000000000008	16,777,21	16,777,216	File	07/18/2008 12:15 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
0000000100000000000000000009	16,777,21	16,777,216	File	07/18/2008 12:17 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
000000010000000000000000000A	16,777,21	16,777,216	File	07/18/2008 12:19 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
0000000100000000000000000005	16,777,21	16,777,216	File	07/18/2008 12:22 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
0000000100000000000000000006	16,777,21	16,777,216	File	07/18/2008 12:25 PM	0.0% /export/home/sdc/nuevo/resources/dbx/pg_xlog/
hast/	0	0	File Folder	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/
nvo_hast_protocol.xml	2,309	2,309	XML Document	07/18/2008 11:49 AM	0.0% /export/home/sdc/nuevo/resources/hast/
ArchiveLabel.xml	1,140	1,140	XML Document	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
MR_256x256.dcm	142,440	142,440	imgfile	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
MR_512x512.dcm	535,162	535,162	imgfile	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
MR_64x64.dcm	19,064	19,064	imgfile	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
cmd_delete	9	9	File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
cmd_pause	17	17	File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/
cmd_remove	37	37	File	06/27/2008 01:49 PM	0.0% /export/home/sdc/nuevo/resources/hast/

Back Up Tool Information continued ...

- **Pull from System** – This button will allow you to save the configuration back up file to a selectable location outside of the server's file-system.
 - If you are connected via a PC on the server's local subnet, you will have the ability to save the file on your PC.
 - If you are connected via a remote connection (Insite/RSvP), you will have the option to save the file to a location on the back-office server using the FFA File Transfer tool.
- **Save on System** – This button will save the configuration back up file to the directory path `/export/backup/system` if the **LKG C** box is **NOT** checked. If the **LKG C** box **IS** checked, it will be saved to :

`/export/backup/last_known_good.`

NOTE

There is no option to save or back-up configuration on a portable media device attached to the server – i.e. **cdrom** or **USB** stick. The **Pull from Server** option pulls the back-up file(s) to a specified file-system location on the client PC system or back-office network you are working from.

ONCE THE BACKUP FILE(S) IS ON YOUR CLIENT PC SYSTEM OR NETWORK - YOU CAN THEN SAVE THE BACKUP TAR FILE TO A PORTABLE MEDIA DEVICE CONNECTED TO THE CLIENT PC SYSTEM YOU ARE WORKING FROM IF YOU DESIRE.

But, there is no direct portable media support for back up on the server itself...

The backup file contains the system ID of the AW Server. This can be used to differentiate several backup files from different AW Server.

The date, time and kind of backup (Users only or System + Users) are also indicated, i.e: AWBUCLAB_backupUser_20140905-154250.tar.gz; AWBUCLAB_backupSyst_20140905-154102.tar.gz

NOTICE

When making a Backup of an AW Server in full or seamless integration mode, the backup must NOT be saved on the system but on a safe location by using the "Pull from system" button.

NOTICE

When performing maintenance/upgrade/backup/restore on clustered AW Servers, note that any server not conforming to current Golden Set will be excluded from cluster. Take this into account when planning your maintenance of clustered servers.

Recurrence

The recurrence section of System configuration backup menu allows to configure the AW Server to regularly backup its configuration at a fixed time.

Recurrence backup is activated by default with a weekly frequency.

- Select recurrence parameters (daily, weekly or monthly) and select "**Activate**" to modify the settings for automated backup.

Automated backup keeps up to the 3 latest backup files, and each backup file contains a time-stamp. The removal of older files is automated and does not impact manual backups.

4.4.2 User Preferences Backup

The tool in this tab was designed to allow individual user preferences and protocols to be saved.

- **Available preferences** – A list of the users that have preferences on the server will be available with check boxes to select them. You can select them individually, or select all of them by checking the box next to User ID.
- **Pull From System** - This button will allow you to save the User Preference configuration files to a selectable location outside of the server's file-system.
 - If you are connected via a PC on the server's local subnet, you will have the ability to save the file on your PC.
 - If you are connected via a remote connection (Insite/RSVP), you will have the option to save the file to a location on the back-office server using the FFA File Transfer tool.

- **Save on Server** - This button will save the User Preference configuration files the directory path /export/backup/system.

NOTE

The User Preference files are saved as part of the System Configuration back up (and the LKGC back up if selected) unless they are de-selected.

NOTE

For details of the Preferences Sharing Manager, see [2.5.4 Preferences on page 98](#).

The screen-shot below is of a listing of the files that are contained in the saved User Preferences back up archive file **for reference only. The actual files, contents and names will depend on the users' names, and their individual preference profiles...**

Use this as a general map to understand what file or files are saved in each general directory path if you are interested in knowing.

If you are viewing this in electronic format, it might be easier to view it if you increase your viewing aspect ratio – magnify the text...

And please be aware that some configuration settings are NOT saved. Notably, the Integration and Scalability parameters, and date and time settings.

Figure 4-6 CONFIGURATION BACK UP FILES EXAMPLE (EXTRACT)

ClientPreferences_admin.properties	0	0	PROPERTIES File	07/18/2008 12:17 PM	0.0% /export/home/sdc/client/prefs/
ClientPreferences_autotest.properties	468	468	PROPERTIES File	07/18/2008 12:16 PM	0.0% /export/home/sdc/client/prefs/
has/	0	0	File Folder	07/16/2008 04:50 PM	0.0% /export/home/sdc/users/
UserPrefs/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/
SdCPreset	3,797	3,797	File	07/16/2008 04:50 PM	0.0% /export/home/sdc/users/has/UserPrefs/
AIA/	0	0	File Folder	07/18/2008 12:26 PM	0.0% /export/home/sdc/users/has/UserPrefs/AIA/
FitterUserPrefs	349	349	File	07/16/2008 08:13 PM	0.0% /export/home/sdc/users/has/UserPrefs/AIA/FitterUserPrefs
FitterLayoutUserPrefs	992	992	File	07/16/2008 08:13 PM	0.0% /export/home/sdc/users/has/UserPrefs/AIA/FitterLayoutUserPrefs
VoxtoolPrefs/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/
protocol/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
images/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/
HEAD/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/HEAD/
PNGs/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/PNGs/
NECK/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/NECK/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/NECK/PNG/
CHEST/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/CHEST/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/CHEST/PNG/
CARDIAC/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/CARDIAC/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/CARDIAC/PNG/
ABDOMEN/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/ABDOMEN/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/ABDOMEN/PNG/
SPINE/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/SPINE/
UPPER_EXTREMITY/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/UPPER_EXTREMITY/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/UPPER_EXTREMITY/PNG/
LOWER_EXTREMITY/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/LOWER_EXTREMITY/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/LOWER_EXTREMITY/PNG/
GENERAL/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/GENERAL/
PNG/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/images/GENERAL/PNG/
HEAD/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
NECK/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
CHEST/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
CARDIAC/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
ABDOMEN/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
SPINE/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
UPPER_EXTREMITY/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
LOWER_EXTREMITY/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
GENERAL/	0	0	File Folder	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
isMyProtocolPrefs.xml	162	162	XML Document	07/18/2008 12:29 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
imageDescription.pref	17	17	PREF File	07/18/2008 12:29 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
layoutPresetOrder.xml	30,727	30,727	XML Document	07/16/2008 08:20 PM	0.0% /export/home/sdc/users/has/UserPrefs/VoxtoolPrefs/protocol/
Voxtool.prefs	184	184	PREFS File	07/18/2008 12:29 PM	0.0% /export/home/sdc/users/has/UserPrefs/
MyTools	610	610	File	07/18/2008 12:29 PM	0.0% /export/home/sdc/users/has/UserPrefs/
VoxtoolJavaUI	121	121	File	07/18/2008 12:29 PM	0.0% /export/home/sdc/users/has/UserPrefs/
ClientPreferences_has.properties	717	717	PROPERTIES File	07/18/2008 12:13 PM	0.0% /export/home/sdc/client/prefs/
backup-list.xml	1,178	1,178	XML Document	07/18/2008 04:16 PM	0.0% /tmp/

NOTE

It is mandatory to save the User Preferences on the active preference server of the cluster.

4.4.3 Configuration backup for Clusters

For clusters of AW Servers, it is recommended to put all the nodes in Maintenance Mode before performing system configuration or user preferences backup. This is intended to ensure that the backup always contains the latest configuration and preferences.

However, it is not mandatory to put all the AW Server nodes in Maintenance Mode.

4.5 Configuration Restore

This menu sub-heading includes two configuration restoration tools as follows.

System Configuration– This tool restores a system configuration from previously-stored system configuration files. The tool shows a list of all available system configuration files. In the “Source” selection area, you can select from:

- “System” (files stored on the system),
- “Upload” (files that have been uploaded to the system from an external computer), or
- “Last known good” configuration files.

Click the “Refresh” button to update the list of files. To delete a file from the list, click the file to select it, then click the “Delete” button.

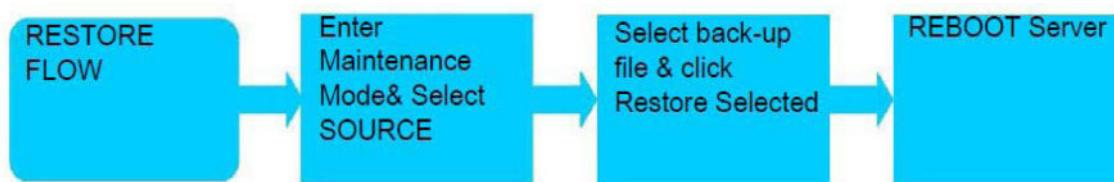
Available configurations

When you click on a file in the list, the “Available configurations” box shows all the configuration items that are available from that file. (A check mark in the box means that the item is available.) Select the desired items from the list by checking or un-checking the boxes.

Comments

The “Comments” box displays comments that were saved with the selected configuration file.

Figure 4-7 RESTORE FLOW OVERVIEW

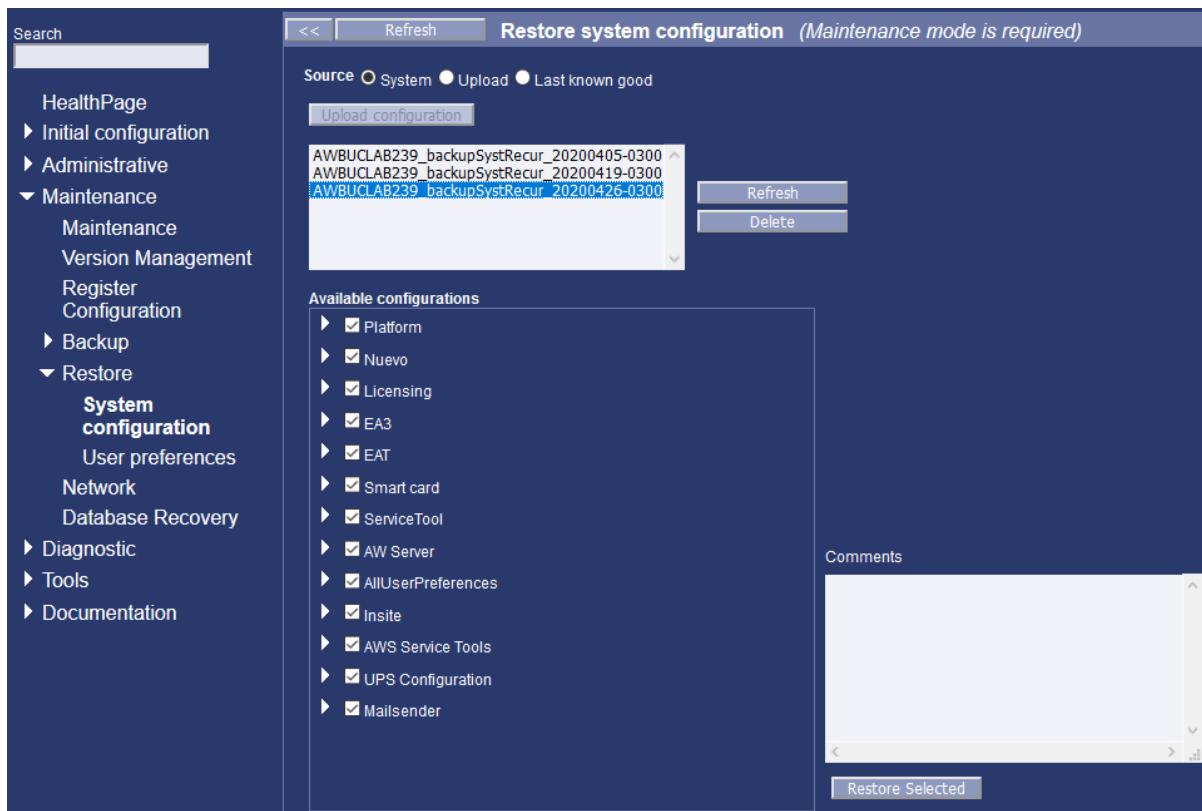


RESTORE- Restore of the system configuration files and user preference files is done through this tool in the **Maintenance Menutree**.

This is one of the server maintenance activities locked into the Maintenance Mode – to ensure corruption-free configuration files – and CANNOT BE PERFORMED WITHOUT USING THE MAINTENANCE MODE.

If you click on the **Restore** link - without first initiating the Maintenance Mode - the “**Restore configuration or preferences**” interface will only display a **Refresh** button, and a message in **RED** letters – **The system is not in maintenance mode operation is not permitted.**

- Select Maintenance in the Administrative Menu, and initiate the maintenance mode – refer and follow the information about Maintenance Mode in the preceding sections of this document.
- You will know that you are in the Maintenance Mode by the **RED** indication at the top of the Service Tools interface (**Maintenance is in progress**), and the Restore tools page will display.

Figure 4-8 RESTORE PAGE**NOTE**

Be careful when using the restore function.

Remember, you will be replacing system or user configuration files with the “last available backed-up versions.”

- The back-up tool will save a listing of the previous backup files.
- So, you will have access to back-up files only as current as the most recent back-up.
- And, you will be able to select from a list of older back-ups if you desire - to test with - or if you have a particular back-up file date in mind that you wish to revert to.

4.5.1 System Configuration Restore

This is the “home” or default tab that is displayed when the Restore tool is accessed. There are several options available for selection or use on this page. **Source** – the source of the restoration configuration file(s).

4.5.1.1 "System" Radio Button

If you select the System radio button, this means that you have elected to restore configuration from the back-up file(s) that have been saved on the server file-system.

- Just below the grayed-out Upload configuration button, there is a PULL-DOWN list of all the server configuration back-up files that exist on the server. These files take the form and location of the following example - /export/backup/system/AWBULAB_backupSyst_20140905-125712.tar.gz
- The system will automatically save some # of these files, and over-write the oldest files, as new ones are saved / backed-up. Notice the date & time code (2008716-154466) of the file names - the most-recent back-up file will be at the bottom of the list.

- Click on the **back-up file** you wish to restore from the pull-down, and use the “**Select**” button - next to the pull-down list – to select that back-up file.
- The “**Select**” button will fill-in the “**Available configurations**” pane - with the appropriate boxes checked - depending on what elements of the configuration are contained in that particular back-up file.
- Finally, click on the “**Restore Selected**” button to initiate the restoration.
- A progress indication will display next to the “**Restore selected**” button, and then a GREEN successful indication – if the restore was successful. If it failed, there will be an error message indicating the failure.

NOTICE

In the case of a failure – notice any actionable messages in the message, and pursue the details - OR –

- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the “**restart**” function from the HealthPage Software Subsystem.
- Reboot the server.
- Reload the platform and/or OS software (LFC).

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

4.5.1.2 "Upload" Radio Button

If you select the Upload radio button, this means that you have selected to restore configuration from back-up file(s) that have been saved in an external file location – like the OLC back-office server, a location on your PC, or a portable media.

- Click on the “**Upload configuration**” button. A small pop-up window (**Send files to server**) will display, presenting the ability to “**Browse**” to a file location, also with a “**Send to AW Server**” and **Cancel** button.
- Browse to the location of the configuration back-up file, select it, and then click the “**Send to AW Server**” button.
- Once the configuration file is sent to the AW Server, it will appear in the “text-box” list - just beneath the Upload configuration button. These files take the location, and form of the following example - `/var/lib/ServiceTools/upload/AWBULAB_backupSyst_20140905-155646.tar.gz`
- Click on the back-up file you wish to restore from the pull-down, and use the “**Select**” button - next to the pull-down list – to select that back-up file.
- The “**Select**” button will fill-in the “**Available configurations**” pane with the appropriate boxes checked, depending on what elements of the configuration are contained in that particular back-up file.
- Finally, click on the “**Restore Selected**” button to initiate the restoration.
- A progress indication will display next to the “**Restore selected**” button, and then a GREEN successful indication – if the restore was successful. If it failed, there will be an error message indicating the failure.

NOTICE

In the case of a failure – notice any actionable messages in the message, and pursue the details - OR –

- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the “**restart**” function from the HealthPage Software Subsystem.
- Reboot the server.
- Reload the platform and/or OS software (LFC).

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

4.5.1.3 "Last Known Good" Radio Button

If you select this server radio button, this means that you have elected to restore the specific configuration from the back-up file(s) that have been saved on the server file-system which automatically include **ALL** available configurations in the back up. The last known good configuration (**LKGC**) is no different than a normal system back up, except for the following specific differences:

- It is designed to always be a complete or total system back up.
- It is saved in its own specific file system location, separate from the normal system back up file - /export/backup/last_known_good/AWBULAB_backupSyst_20140905-153842.tar.gz (this is an “example” file name to illustrate the naming convention)
- It is meant to be a FULL system back up that can be used for system restoration to the last known good configuration after a service or failure scenario that has corrupted or deleted the current configuration.

NOTICE

For a system in Seamless Integration mode, always reload the plugin from the source file before restoring the configuration.

- Just below the grayed-out Upload configuration button, there is a PULL-DOWN list of all the **LKGC** server configuration back-up files that exist on the server. These files take the form of the following example - / export/backup/last_known_good/AWBULAB_backupSyst_20140905-153842.tar.gz
- The system will automatically save ## of these files, and over-write the oldest files, as new ones are saved / backed-up. Notice the date & time code (2008716-154466) of the file names - the most-recent back-up file will be at the bottom of the list.
- Click on the LKGC back-up file you wish to restore from the pull-down, and use the “**Select**” button - next to the pull-down list – to select that back-up file.
- The “**Select**” button will fill-in the “**Available configurations**” pane with the appropriate boxes checked - for the **LKGC** this should be all of them.
- Finally, click on the “**Restore Selected**” button to initiate the restoration.
- A progress indication will display next to the “**Restore selected**” button, and then a GREEN successful indication – if the restore was successful. If it failed, there will be an error message indicating the failure.

- Perform a server **REBOOT** to be sure that all configurations get integrated.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

NOTICE

If the name of a backup file does not contain the string "backupSyst", an error message will appear to indicate that the file name is not correct. The same restriction applies when restoring User Preferences, if the corresponding backup file does not contain "backupUser".

NOTICE

In the case of a failure – notice any actionable messages in the message, and pursue the details - OR –

- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the "**restart**" function from the HealthPage section called Software Subsystem.
- Reboot the server.
- Reload the platform and/or OS software (LFC).

4.5.2 User Preferences Restore

There are a couple of options available for selection or use on this restoration tool. **Source** – the source of the restoration of the User Preference file(s).

System – If you select the System radio button, this means that you have elected to restore User Preferences from the back-up file(s) that have been saved on the server file-system.

Upload – If you select the Upload radio button, this means that you have selected to restore configuration from back-up file(s) that have been saved in an external file location – like the OLC back-office server, a location on your PC, or a portable media.

NOTE

It is possible to restore preferences from another server, via a laptop. However:- Restoring preferences from a previous configuration is not allowed.- It is not recommended to clone preferences between servers, unless explicitly indicated in the AW Server 3.2 Installation and Service Manual, due to potential problems caused by duplicate information.

4.5.3 Final Step after Restore

NOTICE**IMPORTANT FINAL STEP IN SYSTEM OR USER PREFERENCE RESTORE PROCESS.**

There are two levels to determining if the restoration is implemented or not:

1. The restored system configuration shows in the Service Tools sections – HealthPage, device data, contact data, DICOM hosts, Users, Licensing, and so on ...
2. The system configuration is available in the client application when the user connects to the server. Essentially this means – does the "system" work?

There is no ONE-way to determine if the restoration was completely successful by examining any ONE thing in either of these TWO operational levels.

TO RELIABLY RESTORE THE BACKUP REBOOT THE SERVER AFTER THE RESTORE IS COMPLETE. IF YOU DO NOT, THERE IS A RISK THAT THE RESTORE WILL FAIL PARTIALLY OR TOTALLY.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

4.5.4 Summary of restore behavior

For a table describing the behavior of Service Tools when restoring a system configuration file, refer to the AW Server 3.2 Installation and Service Manual, System Configuration Restore Matrix.

4.5.5 Configuration restore for Clusters

For clusters of AW Servers, it is mandatory to put all the nodes in Maintenance Mode before performing system configuration or user preferences restore. If one or several nodes of the cluster are not in Maintenance Mode, the restore might result in corruption of system configuration and/or user preferences.

Therefore a configuration restore implies a downtime for the whole cluster. This downtime should be planned at a time of low activity.

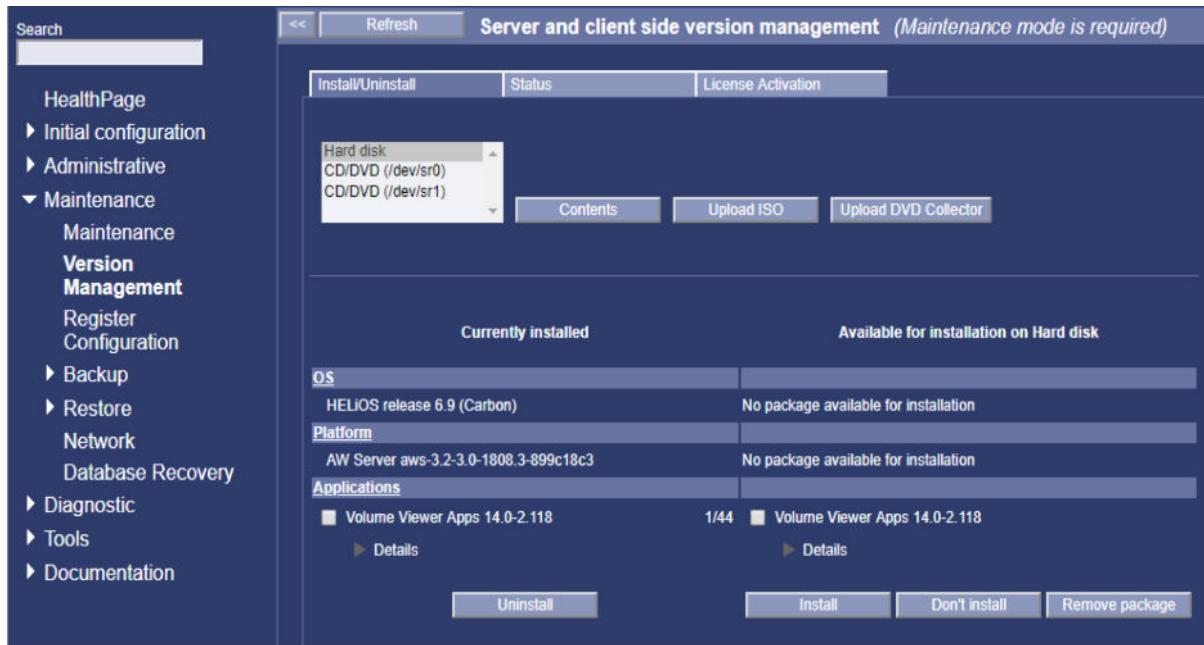
When restoring an "old" backup file, take into account that it will overwrite all new user preferences that were modified since the backup, for all nodes in the cluster. If you decide it is more appropriate, do not restore the user preferences. This can be done by unchecking "AW Server" and "AllUserPreferences" in the restore menu.

4.6 Version Management

Use this tool to show which software versions are currently installed for the OS, platform, and applications, and to see which installations are available for installation on the server's hard drive and media drive. You can use the tool to uninstall existing software and install new software. Application updates are not deployed by GERU for AW Server 3.2. The "Status" tab shows the current status of any software installation/uninstallation tasks

4.6.1 Version Management Tool Example

The actual versions you will have on your screen may vary from the below example.

Figure 4-9 VERSION MANAGEMENT TOOL EXAMPLE

4.6.2 Version Management Tool

The home page of the Version Management tool is the **Install/Uninstall TAB**.

The second **TAB** in the **Version Management** tool page is the “**Status**” tab. This tab displays an interface where the uninstall and install status and error message are logged.

4.6.2.1 Install/Uninstall TAB.

The Install/Uninstall Tab is divided into **FOUR** horizontal sections. Also, right and left columns listing the AW Server **CURRENT contents** on the **LEFT**, and the **Contents** of the selected **DEVICE** on the **RIGHT**.

- The **TOP** section essentially defines the method to select a package for installation.

Hard disk or CD/DVD selection window:

- Click to select **CD/DVD** if the file(s) to load are delivered on a CD or a DVD media
- Click on **Hard disk** if the file(s) are already available on the hard disk or on USD media.

Contents – This will fill in the right column with the contents of the selected device – if the device contains a package on it that the tool can recognize.

Upload iso - This will open a pop-up to browse to the location of an application iso file. The selected iso file is uploaded to the hard disk of the AW Server, but it is not installed. This is especially used for Virtual Machines. It is possible to indicate the md5sum of the iso to ensure that transfer did not corrupt the file.

Upload DVD Collector - This is similar to upload iso, however it allows to upload multiple files at the same time. This is used with the DVD Collector which contains several application iso files and their corresponding md5sum files. Browse to the DVD Collector location, select all files and upload them. The upload is done in parallel.

NOTE

Software load through USB device. When installing from electronic files, always refer to **5761599-8EN: AW eDelivery Service Guide** for detailed instructions.

1. ***Currently installed*** section

- Next to the top section displays the **OS** package **Name** and **Version**. The **LEFT** side is the currently installed package, and the **RIGHT** side is the OS package detected on the selected device – if it exists.
- Next to the bottom section displays the **PLATFORM Name** and **Version**. The **LEFT** side is the currently installed package, and the **RIGHT** side is the platform package detected on the selected device – if it exists.
- The **BOTTOM** section displays the **Name** and **Version** of the **Advanced Applications Packages** currently on the server. The **LEFT** side is the currently installed package(s), and the **RIGHT** side is the advanced applications package(s) detected on the selected device – if they exist.
- For the applications that are ‘licensable,’ the software and eLicense “**license string**” is shown beneath the name, and a little to the right.
- For embedded applications that do not require a license, the notation “**No License Required**” appears.

In the BOTTOM “**Applications**” section there is also an **Uninstall** button – This button will uninstall the selected advanced application(s). **MUST BE IN MAINTENANCE MODE TO UNINSTALL**

2. ***Available for installation on Hard disk*** section

- Next to the top section displays the **OS** package **Name** and **Version**. The **RIGHT** side is the OS update package detected on the selected device – if it exists.
- Next to the bottom section displays the **PLATFORM Name** and **Version**. The **RIGHT** side is the platform update package detected on the selected device – if it exists.
- The **BOTTOM** section displays the **Name** and **Version** of the **Advanced Applications Packages** currently on the server. The **RIGHT** side is the advanced applications package(s) detected on the selected device – if they exist.
- For the applications that are ‘licensable,’ the software and eLicense “**license string**” is shown beneath the name, and a little to the right.
- For embedded applications that do not require a license, the notation “**No License Required**” appears.

In the BOTTOM “**Applications**” section there are also the following buttons:

- **Install** – This button will install the selected applications package file(s).

MUST BE IN MAINTENANCE MODE TO INSTALL

- **Don't install** - this button will NOT remove the selected package file from the device, but will move it to another directory, where it can be retrieved if necessary.
- **Remove package** – This button will permanently remove the selected package file from the hard disk.

NOTE

Previous versions cannot be reinstalled directly. Need to uninstall the currently installed version first.

4.6.2.2 Status TAB

The second **TAB** in the **Version Management** tool page is the “**Status**” tab. This tab displays an interface where the uninstall and install status and error message are logged.

4.6.2.3 Synchronization of Versions on a Cluster

In case of cluster configuration, any modification of the version on one AW Server will make the node non-compliant with the Golden Set of software. Therefore, the modification must be made on ALL nodes of the cluster, and the Golden Set will have to be reset.

4.6.2.4 Register Updated Configuration

After any modification of the software version on AW Server, you must send the updated configuration AW Back Office by email. Refer to Chapter 5, [5.3.8 Registration on page 429](#).

4.7 Network Reconfiguration

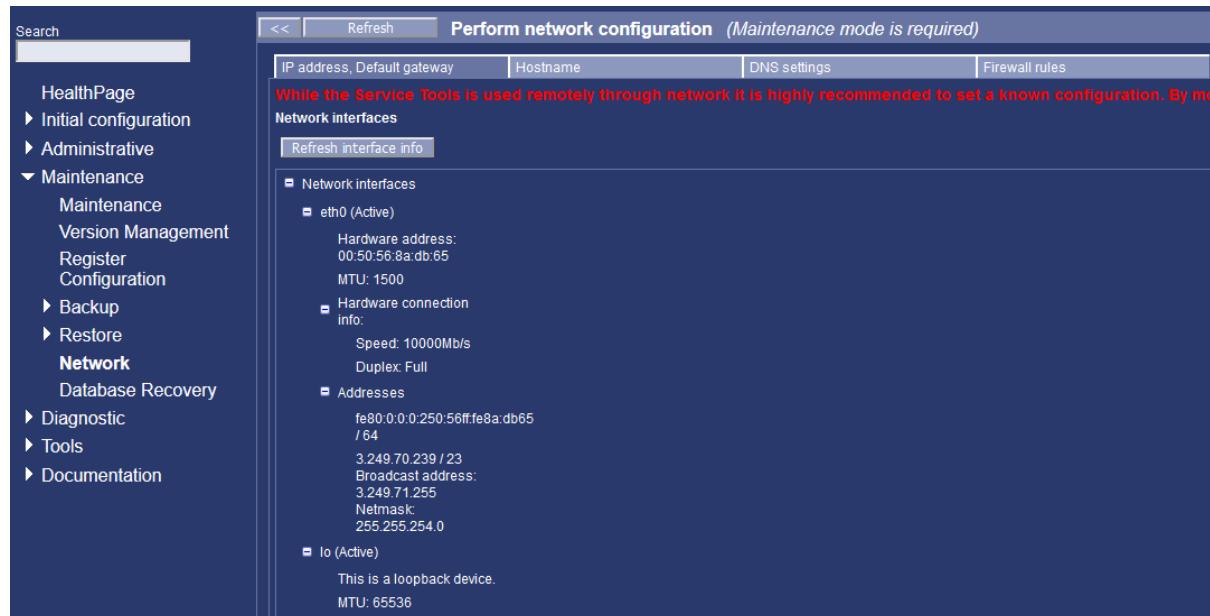
The AW Server Network parameters can be reconfigured, if necessary by the Service user or the Administrator, directly from the Client PC, under the **Maintenance** mode.

NOTICE

Changing the network configuration (IP, Default gateway) is a serious step. If the configuration is mistyped or erroneous, the user will no longer be able to connect to the server. Keep in mind that reconfiguring the Network parameters of the AW Server will have the following effects:

- Entering the Maintenance mode will disconnect all the Users.
- Once reconfiguration is done, clicking on the **Apply** button will disconnect you (Service or Administrator user) from the server
- New configuration (IP address) will have to be taken into account for all the Client PCs
- Remote service will no longer be possible, until a new Checkout is done.

The following is an example of the configuration screen

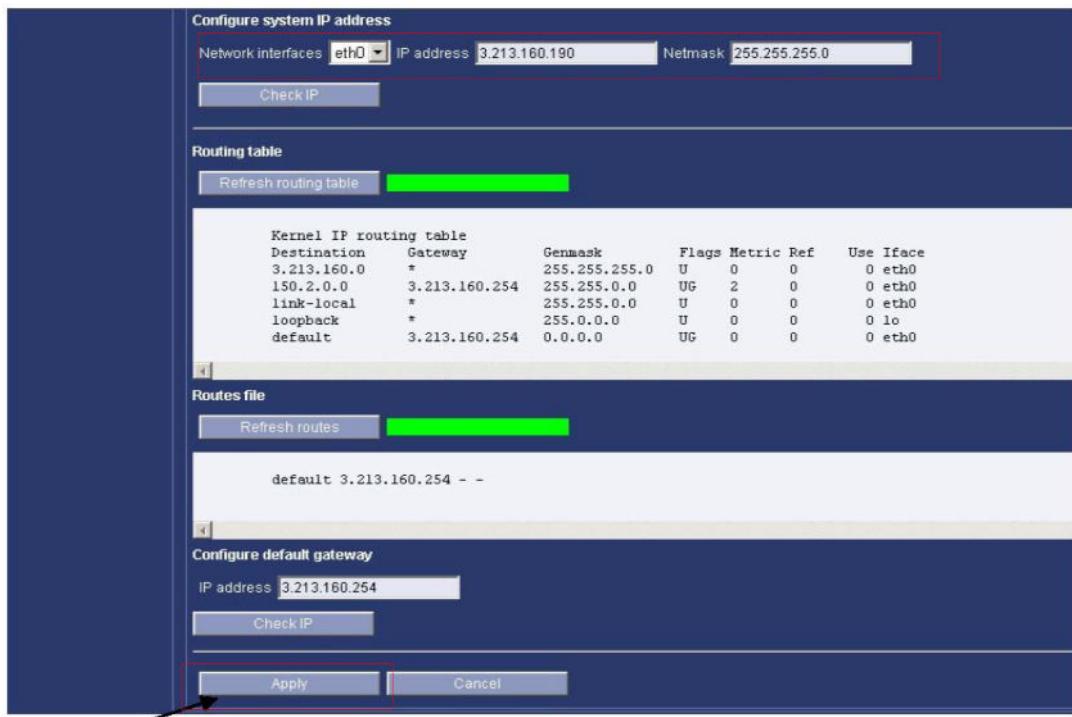


4.7.1 IP Address, Default Gateway

The first tab on this screen allows changing the AW Server IP address and Netmask/Network Prefix, as well as the Default Gateway IP address and Netmask/Network Prefix.

It also displays the current hardware and configuration characteristics of the “active” server network ports. This is mostly self-explanatory and is similar to the information that can be captured at command-line with the **ifconfig** command:

Scrolling down gets you the AW Server and Default Gateway IP and Netmask/Network Prefix settings.



Configure System IP Address

Use this to check or change the system’s IP address and Netmask/Network Prefix. Click the **Check IP** button to see if the IP address is valid.

NOTE

At least 2 IP addresses have to be configured and checked in case of a cluster of AWServers.

Routing Table

This section displays the current routing table information for the AW Server.

Routes File

This section displays the current routes file for the AW Server.

Configure Default Gateway

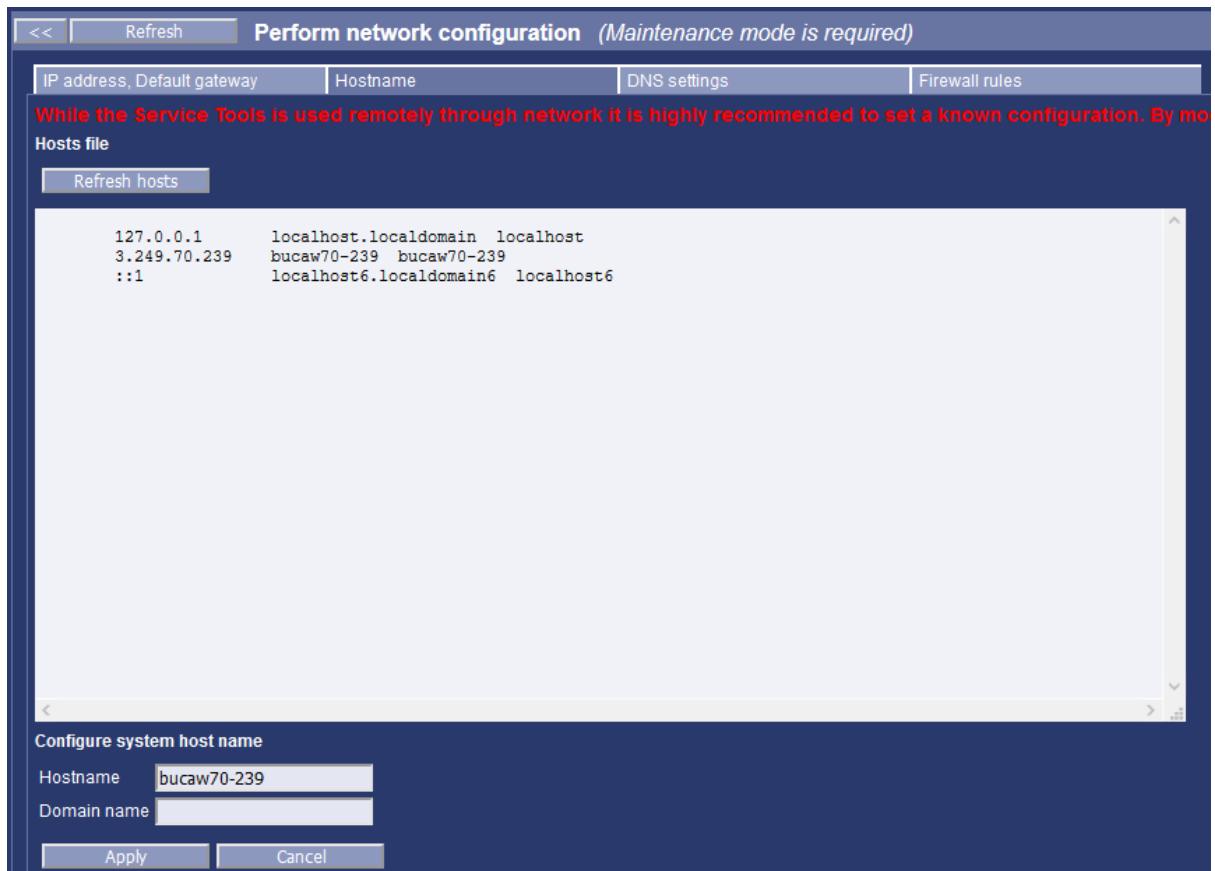
This section displays the current gateway for the AW Server, or you can enter a different gateway address, then click the **Check IP** button to see if the IP address is valid.

Saving the Changes

If you have entered any changes for this page and want to save them, click the **Apply** button at the bottom of the page.

4.7.2 Hostname

The second tab allows changing the AW Server hostname.

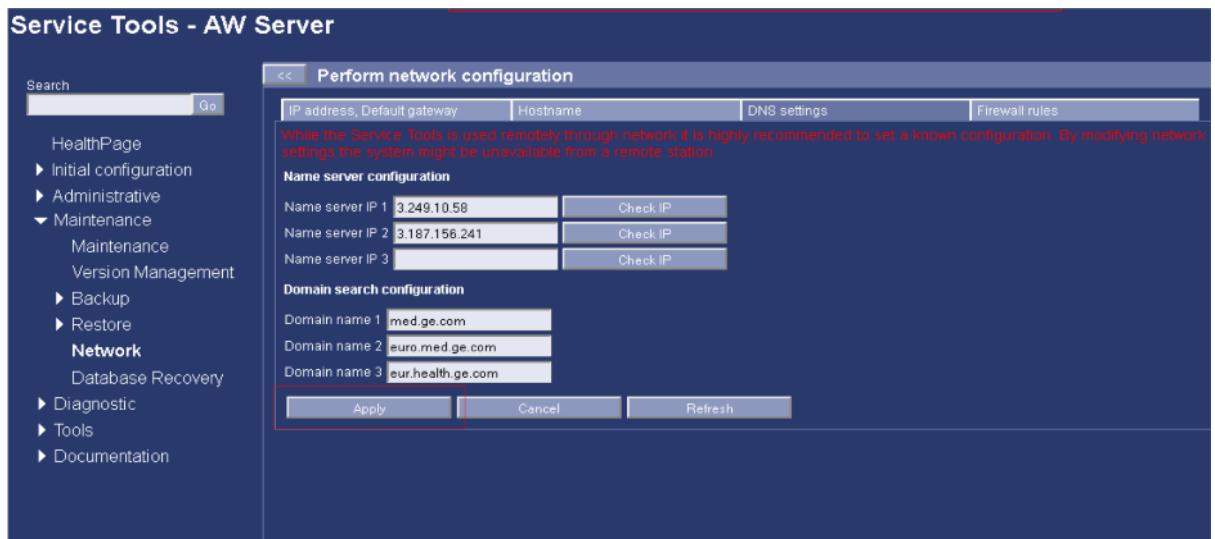


- Enter the new Hostname in the *Hostname* field and click on the **Apply** button.

4.7.3 DNS Settings

The third tab provides a mean to configure Name servers and Domain servers via the Service Tools (as an alternative to the Linux command line). Use with caution.

Example configuration:



- Enter the DNS server(s) configuration data and click on the **Apply** button.

4.7.4 Firewall Rules

The fourth tab is informational only and does not allow modifying the AW Server Firewall settings.

```

<< Refresh Perform network configuration (Maintenance mode is required)
IP address, Default gateway | Hostname | DNS settings | Firewall rules
Firewall rules
Refresh firewall info

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 612K 86M ACCEPT all -- lo any anywhere anywhere state
 6996 843K ACCEPT all -- any any anywhere anywhere state
RELATED,ESTABLISHED
      0 0 ACCEPT all -f any any anywhere anywhere
      2343 118K BAD_FLAGS tcp -- any any anywhere anywhere state tcp
      1999 97036 SYN-FLOOD tcp -- any any anywhere anywhere state tcp
flags:FIN,SYN,RST,ACK/SYN
      0 0 DROP all -- any any 255.255.255.255 anywhere
      478K 41M PNF_DYN all -- any any anywhere anywhere state tcp
      477K 41M DROP all -- any any anywhere anywhere state

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 621K packets, 94M bytes)
pkts bytes target prot opt in out source destination

Chain BAD_FLAGS (1 references)
pkts bytes target prot opt in out source destination
      0 0 LOG tcp -- any any anywhere anywhere limit: avg 1/min
burst 5 tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,PSH,URG LOG level warning prefix 'PNF:KAS XMAS FLAG: '
      80 4800 DROP tcp -- any any anywhere anywhere state tcp
flags:FIN,SYN,RST,PSH,ACK,URG/FIN,PSH,URG
      0 0 LOG tcp -- any any anywhere anywhere limit: avg 1/min
burst 5 tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,ACK,URG LOG level warning prefix 'PNF:KAS MERRY XMAS FLAG: '
      0 0 DROP tcp -- any any anywhere anywhere state tcp
flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,ACK,URG
      0 0 LOG tcp -- any any anywhere anywhere limit: avg 1/min
burst 5 tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN LOG level warning prefix 'PNF:KAS FIN FLAG: '
      0 0 DROP tcp -- any any anywhere anywhere state tcp
flags:FIN,SYN,RST,PSH,ACK,URG/FIN
      0 0 LOG tcp -- any any anywhere anywhere limit: avg 1/min

```

Fire-wall rules configuration display is the output from the command **iptables -L** (or use --help option with the command to see other options)

Each line represents a rule in the firewall.

For each rule, the following information is shown:

pkts: the number of IP packets handled by the given rule

bytes: the number of bytes handled by the given rule - the size of all packets summed

target: what does this rule do with the matching packets

prot: the network protocol to match - udp, tcp, etc...

opt: further options to match

in: the incoming network interface to match

out: the outgoing network interface to match

source: the source of the packet to match

destination: the target of the packet to match

other options: any further options

PNF has two modes of operation: **ON** and **OFF**.

- In the **ON** state/mode, PNF will allow only the network communications that are specified by its configuration and reject all the rest.
- In the **OFF** mode, PNF will allow all communication (subject to only the filters set by the modality script).

NOTICE

If the PNF Firewall is turned off, and left off, this will introduce the server to a security risk. Malicious users can login via SSH and access, corrupt, or delete sensitive files. The server can be used for unauthorized purposes. Vulnerability scans will fail... etc...

The mode can be changed using the manager CLI, and is persistent across reboots.

Refer to Chapter 3 for further details.

4.7.5 Network Interface Information

Command-line “**ifconfig**” example output:

eth0

Link encap:Ethernet **HWaddr 00:1B:24:78:C4:98**
inet addr:3.57.48.64 Bcast:3.57.51.255 Mask:255.255.252.0
inet6 addr: fe80::21b:24ff:fe78:c498/64 Scope:Link
UP BROADCAST RUNNING MULTICAST **MTU:1500** Metric:1
RX packets:336607 errors:0 dropped:0 overruns:0 frame:0
TX packets:23296 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:32368962 (30.8 Mb) TX bytes:5788585 (5.5 Mb)
Base address:0x8c00 Memory:fc6e0000-fc700000

lo

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING **MTU:16436** Metric:1
RX packets:10222 errors:0 dropped:0 overruns:0 frame:0
TX packets:10222 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3824842 (3.6 Mb) TX bytes:3824842 (3.6 Mb)

	Interface Info
--	----------------

Server public or applications network port Network Card MAC (Media Access) address Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet transmitted... Speed capability & Bi-Directional flow IPA of applications port Built-in Loop-back Diagnostic port configuration	Interfaces eth0 (Active) Hardware address: 00:1B:24:78:C4:98 MTU: 1500 Hardware connection info Speed: 1000Mb/s Duplex: Full Addresses 3.57.48.64 / 22 Broadcast address: 3.57.51.255 lo (Active) This is a loop-back device. MTU: 16436 Failed to get hardware connection information. CONNECTION SPEED AND DUPLEX INFORMATION IS NOT AVAILABLE FOR THIS INTERFACE LOOP-BACK DEVICE. Addresses 0:0:0:0:0:1%1 / 128 127.0.0.1 / 0
---	--

4.8 Database Recovery

The Database Recovery function can be used to rebuild the server's image database after a load-from-cold.

NOTE

This procedure does not apply for AW Servers in Seamless or DICOM Direct Connect integration, because the database is stored on the PACS.

NOTICE

DATABASE RECOVERY WARNING.RISK OF MISDIAGNOSIS DUE TO INCOMPLETE DATA SETS!

When a server software reinstallation is completed (load-from-cold), the image database is retained and rebuilt after the platform software is installed. This means that if there is a large database retained, the rebuild of the database could take a long time.

- **Average image install rate is 100 images/second** (up to 512x512 image sizes). Assuming this rate, it will take about **14 hours** for 5 million images and about **45 hours** for 16 million images

Be aware: If the complete data set is not reloaded before you turn the server over to the customer, users can access the server and could access INCOMPLETE DATASETS!

To avoid the risk of mis-diagnosis due to incomplete datasets, do the following:

1. Make sure - for the duration of the DB Rebuild - that the users are aware of this potential situation. Use the Service Tool Client Broadcast Messaging Tool to set the following message for end users as soon as possible after the server is ready to be accessed:

"WARNING – DATABASE RECOVERY IS IN PROGRESS. INCOMPLETE DATASETS MAY BE DISPLAYED IN THE BROWSER. PLEASE CONFIRM THE NUMBER OF IMAGES IN A GIVEN DATASET BEFORE LAUNCHING AN APPLICATION."

2. Monitor the DB rebuild by monitoring the following logfiles in the log-viewer tool – until the rebuild is complete.

- Platform Nuevo: DB recovery log (nuevo)
 - Platform Nuevo: DB recovery output (nuevo)
3. Be sure to close the broadcast message when the DB recovery / rebuild is complete, to allow normal system use again.

Database Recovery – This is another tool that is locked into the **Maintenance Mode** tasks. That is, if you attempt to start the DB recovery without being in **M-MODE**, it will indicate that you must be in Maintenance Mode to perform a Data Base Recovery.

NOTICE

USE THIS TOOL ADVISEDLY. THE AW SERVER CAN CONTAIN “TERABYTES” OF IMAGE DATA. A DATABASE RECOVER COULD TAKE A LONG TIME AND COULD INADVERTANTLY CAUSE OTHER SERIOUS PROBLEMS IF THERE IS A SYSTEM FAILURE OR INTERRUPTION WHILE IT IS TAKING PLACE.

- The database recovery time depends on the number of the DICOM objects stored in the database.
- The recovery on a full database may take 15 - 30 hours depending on the number of used DICOM objects!
- Inform the customer that the image recovery / reinstall process could go on for a long time (as noted above) & during that time there will be no user(s) access - due to Maintenance Mode Lock-Out. There is no way to ensure complete data availability during a DB rebuild, so the server should not be used until the DB is complete.
- **Average image install rate is 100 images/second** (up to 512x512 image sizes). Assuming this rate, it will take about 14 hours for 5 million images and about 45 hours for 16 million images
- **Do not reboot the server during a database recovery**, otherwise data loss will occur.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- **The Service Tools should not be taken out of Maintenance Mode while the recovery is in progress**, and this until completion.
- **The Service Tools login timeout should not come into play during a DB recovery**, since the Service Tools servlet client gets refreshed every 3rd sec with a new status from the DB server.
- **The recovery status and history can be viewed in the /export/home/sdc/nuevo/logfiles/recoverDB.log**

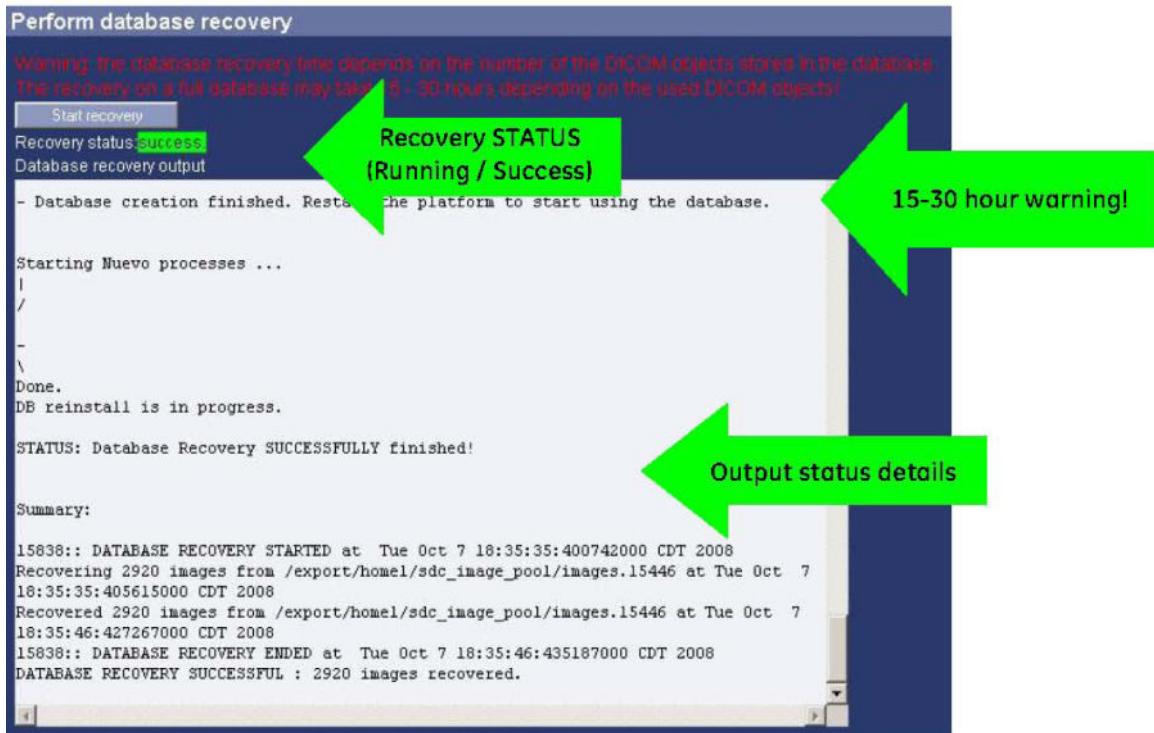
There are 2 KNOWN cases when a database recovery is needed:

1. Sequence ID of Postgres crosses the limit (9223372036854). This essentially maps to number of rows in the database tables. So if the system had installed 9223372036854 patients or 9223372036854 studies or 9223372036854 series or 9223372036854 images – then the database needs to be recovered to reclaim any unused sequence ID in-between.
2. There was an inconsistency detected between the postgres tables and the DICOM composite files stored under \$SdC_IMAGE_POOL/images directory.

NOTICE

Both of these cases are checked for during the database startup and a recovery is initiated automatically.

- **A database recovery is automatically accomplished during all OS or Platform (LFC) software installations.**
- This information is pretty much for your “information” sake only. You should not see very many reasons or situations where a database recovery is needed...
- Do not use this tool as a catch-all – if you use it at all



NOTE

After a database recovery, it is recommended to check the following folder does not contain too many images, as this may cause disk availability issues on the partition. Open a terminal and type:

- `cd /export/home1/sdc_image_pool/failed_to_reinstall/ <Enter>`
To check the utilization of this folder type
- `du -sk . <Enter>`

According to the results (displayed in kb), you may reinstall, delete, or simply leave the images as they are. Reinstallation is normally recommended - contact your OLC for details.

4.9 Register Configuration

The use of Register Configuration after AW Server and Applications installation is detailed in the AW Server 3.2 Installation and Service Manual. Below is a description of service procedures for Configuration Registration-related actions.

The url for the AWCCT Website is from the Internet: <https://awcct.gehealthcare.com>. This url will replace the former url <http://awcct.health.ge.com>.

4.9.1 Troubleshooting Configuration Registration

While performing the Configuration Registration, you might face the situations or questions described in this section.

4.9.1.1 Different values for Permanent Key

Each time a configuration file is uploaded to the AWCCT website, a new registration key is calculated. The new registration key is valid, and the previous registration key is also valid. The consequence is that it is possible to have more than one valid Permanent Key for a single system. In other words, there can be different values for Permanent Key for a given system.

4.9.1.2 Configuration files with no extension

The AWCCT Website does not support the upload of configuration file with no extension, or with extension different from ".txt".

Do not change the file extension when generating the configuration file on AW Server.

4.9.1.3 Backup/restore of registration key

The registration key is part of system configuration backup and restore mechanism. To backup or restore the registration key, refer to [4.4 Configuration Backup on page 394](#) and [4.5 Configuration Restore on page 401](#).

Note that the registration key will not be restored if it is not valid for the target system.

4.9.2 Configuration Registration command lines

When the Service Tools Configuration Registration menu is not accessible, you can use the following command lines in a terminal or in an ssh session.

NOTE

ICM is the internal name of the Configuration Registration feature. The command lines below are therefore named "icm". When searching the system for information related to Configuration Registration, you can use the "icm" keyword.

4.9.2.1 setKey

/usr/bin/icm --setkey <REGISTRATION_KEY> <Enter>

e.g.: /usr/bin/icm --setkey 0123456789a

This command enables to set the registration key. The parameter <REGISTRATION_KEY> is the 11 characters key returned by the AWCCT Website. If no registration key is provided or if an invalid registration key is provided an error message will be returned.

4.9.2.2 doAutoRegister

/usr/bin/icm --doAutoRegister <Enter>

If the AW Server is remotely connected (InSite/RSvP), this command performs auto registration. A report is registered at /export/home/sdc/icm/icmregistrationreport.

4.9.2.3 version

/usr/bin/icm --version <Enter>

This command returns the version of the ICM component, providing the Configuration Registration feature. This value is a shorter string than the one displayed in the HealthPage in the Version Information section for ICM.

4.9.3 Configuration Registration logfile

When investigating issues with Configuration Registration, consult the following logfile on the AW Server:

```
/export/home/sdc/logfiles/icmlog <Enter>
```

This logfile can be viewed using the **Service Tools > Diagnostic > Log Viewer** menu. Use the keyword **icm** to search for this logfile.

Alternatively, you can use the following command lines to view the logfile in a terminal.

```
cd /export/home/sdc/logfiles <Enter>
```

(This command line is equivalent to `cd ~sdc/logfiles <Enter>`)

```
less icmlog <Enter>
```

4.9.4 Configuration Registration Call Center

In case of questions related to Configuration Registration process, you can contact the Configuration Registration Call Center. Please call:

- +1 855-741-3136 (toll free number for US only.)
- +1 262-524-5660 (if the first phone# does not work)

This Call Center will not provide registration key. Its purpose is to provide support on the usage of Configuration Registration.

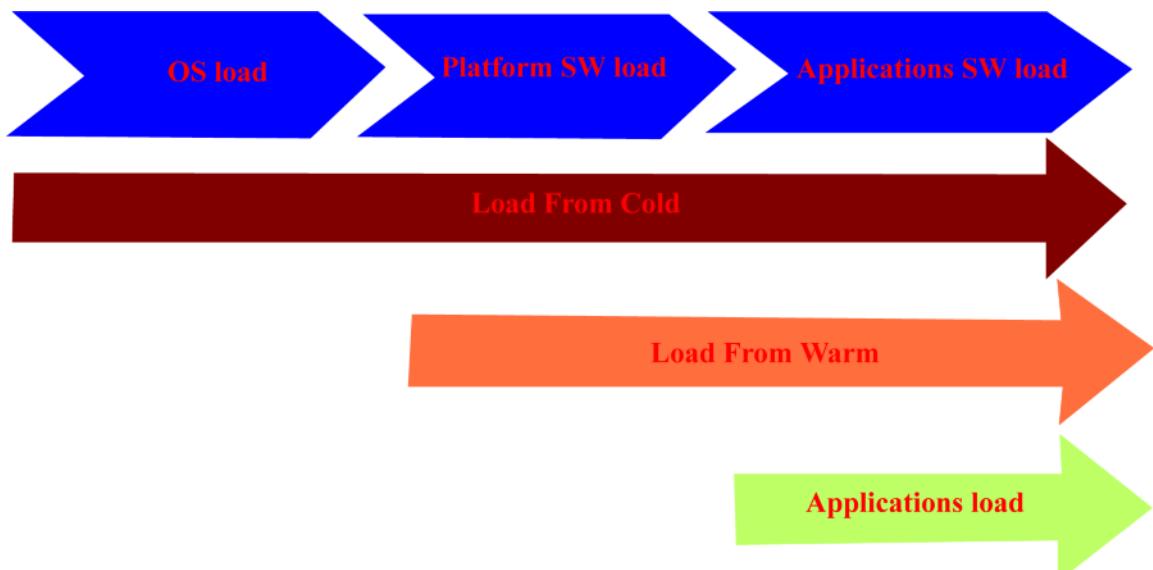
Chapter 5 Software Reload and Client Reinstall

5.1 Overview

This chapter covers the following items:

- Section [5.2 Software Load Process on page 419](#)
- Section [5.3 Additional Software Load information on page 420](#)
- Section [5.5 AW Server Client Software Upgrades on page 433](#)

Figure 5-1 SOFTWARE INSTALLATION FLOW



For the initial installation of new Forward Production Hardware servers, the system is factory preloaded with OS, Platform and Applications. For other Hardware initial installation and for upgrades, the GE FE has to install steps 1, 2 and 3

NOTICE

The Volume Viewer Apps software may not be factory pre-loaded. When it is the case, a warning sticker on the server packaging notifies it.

5.2 Software Load Process

Detailed software load steps are not covered in this chapter. See instead, the following sections of the AW Server 3.2 Installation and Service Manual:

- Quick Start Installation Guide - Physical AW Server or Quick Start Installation Guide - Virtual AW Server, in particular the Software load flowchart.
- Job Card UPG001 - Software Upgrade for standard software upgrade procedure.
- Job Card UPG003 - Hardware Upgrade for hardware upgrade procedure.

NOTICE

For upgrades, it is recommended to follow the full Load From Cold procedure (complete SW reload including OS).

NOTICE

There are special considerations when reloading / upgrading software on a Virtual AW Server that is configured as part of a scalable "cluster".

NOTICE

For Virtual AW Server, the reload of software must be done using the existing Virtual Machine. No new Virtual Machine must be created to load the software.

NOTICE

The list of applications compatible with AW Server is subject to change as new releases are regularly made available. Refer to the Compatibility Matrix for the detailed list of compatible applications. The Compatibility Matrix is available as DOC0692114 in MyWorkshop and on SIMS Content Viewer.

NOTICE

When upgrading an AW Server 2.0 to AW Server 3.2, if you plan to upgrade the filesystem for image and backup partitions to Ext. 4, DO NOT FORGET TO PULL FROM SYSTEM THE SYSTEM CONFIGURATION BACKUP. The reason is that all backup files stored on the AW Server itself will be lost when upgrading to Ext. 4. Therefore it is critical to backup the system configuration on an external system (GE Laptop, Customer PC).

NOTICE

To set the hostname, refer to the rules in the AW Server 3.2 Installation and Service Manual, Specific field - Characters rules and limitations.

Once the network parameters have been setup, you can see the result by typing:

cat /etc/hosts <Enter>

Example 1 of /etc/hosts file:

192.0.4.25 aws-06 aws-06

This is the hostname of the NIC card and 192.0.4.25 the IP address of the AW Server.

Example 2 of /etc/hosts file:

192.0.4.25 aws-06.euro.health.ge.com aws-06

where aws-06 is the hostname of the NIC card, euro.health.ge.com is the domain name and 192.0.4.25 the IP address of the AW Server.

5.3 Additional Software Load information

This section gives additional information on software load related topics, such as the backup and restore processes, or currently known issues and workarounds.

5.3.1 Load From Cold (LFC) Considerations

The OS (operating system) installation on this product is considered a **Load-From-Cold** process. This means that it is the most significant software intervention that can be done on the system. It is the first step in an initial system build or re-build of the entire software system. As a consequence, it resets and/or removes all previous user configuration parameters and files, and replaces them with "system defaults."

On Hardware server with a separate Disk Array Storage, the LFC does NOT remove or replace the IMAGE files from their image partition – they are retained unless there is a related hardware failure with the image partition. Additionally, the backed-up AWS system configuration files are also retained in the image partition for availability after any load-from-cold intervention.

On Virtual Machines, the **LFC** also keeps the image partition and the backed-up AWS system configuration files, if the Virtual Machine has 2 virtual hard disks.

The OS installation process takes about 25 to 35 minutes to complete.

After about 15 minutes, user interventions will be required again, in order to complete the OS loading.

The OS for this product is based on Scientific Linux OS (HELiOS). It is essentially an off-the-shelf package with an automated configuration script - which automatically sets needed installation parameters for this product.

The OS version is indicated on the media label. You can also verify the OS version indicated in the following locations:

- In the file called `release.txt` on the Operating System media. You will see a value similar to: `AWS3.2_OS_5.1` (or higher)
- In the name of the OS template file.

After installation, you can check the OS version installed on the Service Tools HealthPage.

NOTE

Once the installation begins, no intervention is required until you need to configure the date and time and then load the AW Server platform media. The OS installation takes about 25 minutes to complete.

5.3.2 Installation failures

NOTE

If any of the packages show a FAILURE indication, there is likely something wrong, and the platform software installation is not completely successful.

- Make a note of the failed package(s)
- Examine the media, and make sure it is not scared or dirty, then restart the platform installation from the beginning.
- If it fails again the possibility is that the media might be faulty, or the media drive might be faulty. If the drive functioned without error in the OS load, then it is most likely is OK.
- Acquire a new media FRU of the platform software – see FRU section. If a new media still fails, perhaps attempt the load-from-cold of the OS again from the beginning.
- Once the media and OS process is eliminated as the cause – a reasonable course of action might require hardware diagnostics to be run on the server. For the High Tier servers, this is a Hardware Vendor activity, and the break/fix process (see [Chapter 1, 1.4 Service Model and Break-Fix Processes on page 46](#) should be engaged to get this going. **This means the Vendor must be called to come in and do the diagnostic analysis and repair of a potential**

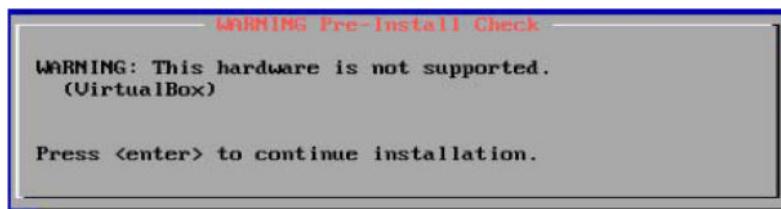
hardware problem. In a case like this, it is required that GEHC stay closely engaged with the Vendor during this process to be available for any actions that might involve software activity, and to coordinate the final fix.

5.3.2.1 Unsupported Hypervisor Hardware case

Refer to the AW Server 3.2 Pre-Installation Manual, Requirements for Virtual AW Server to know the virtualization platforms (hypervisors) supported by the AW server.

Installation of the virtual AW Server is authorized on unsupported Hypervisor Hardware type, but an acknowledgment message will be displayed when loading the AWS Platform software, to warn the GEHC Field engineer that this type of hardware is not supported.

See example below:



- Press <Enter> to continue with the installation

The installation will proceed as usual, but when complete, the HealthPage will show in the *Machine* typefield, the name of the unsupported Hypervisor HW, in order to highlight that any erratic behavior of the AW Server software might be caused by this unsupported Hypervisor.

Image partition mount count (Current / Max.)	Not applicable
Image partition next file system check date	Not applicable
Certificate expiration date	Mon 02 May 2022 11:07:54 AM CEST
Clam AV Antivirus Software status	Not activated
Machine type	VirtualBox VirtualBox 5.0.24 Unsupported version!
Install mode	server
DICOM AET (printing)	
Service Processor	N/A

5.3.3 Platform Licensing

NOTE

The 8,000, 16,000, 40,000, 80,000, 160,000 slice license is roughly analogous to the SdC license on the AW platform. It is needed in order for the client user to be able to access the advanced applications in the AW Server client browser interface. The High Tier server hardware is exactly the same for both the 16,000 and 40,000 (prior to Q3 2016) or 16,000, 40,000, 80,000, 160,000 (from Q3 2016) slice licensed configurations. The only difference is in the functionality. No hardware is needed to upgrade from the 16,000 to the 40,000 or to 80,000, 160,000 (from Q3 2016) slice product – only the AW Server Upgrade **16,000 (FOUR seat) to 40,000 Slices (EIGHT seat)** or to **80,000 (High Tier Standard)** or to **160,000 (High Tier Premium)** license.

Only the 8,000 slices (TWO seat) or 40,000 (EIGHT seat) licenses are available for the virtualized AW Server (non-integrated). However, it is fixed to 16,000 slices for Seamless integration with the Universal Viewer, and 40,000 slices for DICOM Direct Connect integration. For DICOM Direct Connect integration in CT Nano-Cloud environment it is fixed to 4,000, 12,000 or 16,000 slices.

The eLicense web-site is setup to create these keys. The Global Order Number (GON) should identify clearly which product has been purchased in terms of a slice license catalog. See also **A.2 AW Server Licensing on page 469** and for further information see the **AW eLicense User Guide** (Part No. 45462232-100) available via the User Guide link on the eLicense website @ <http://elicense.gehealthcare.com/elicense/>

The following **Model Types** are available for AW Server 3.2:

- **AWS_Primary:** Use instead of **AWS** when new server hardware is shipped. When in a Virtual configuration the CoLA License server and all of the applications will be licensed to this hostID.
 - **AWS_Node:** In a Virtual environment, the Node-locked licenses (# seats License, Autolaunch, (PreProcessing), Integration) are assigned to each hostID of each node for the scalable system.
- The hostID for an **AWS_Primary** system can also be one of the assigned nodes. In this case, that particular node would look just like a physical server system, as all of the licenses would be assigned to the same hostID.
- **PC_APP:** Currently applies only to a workstation on which the new application CortexID Suite is installed. Enter the hostID (MACID) of a PC that will have this application installed on, to get the appropriate licenses. Other applications may move to this format in the future and will then be enrolled under this model-type.

The initial license key installation must be manually entered – either during the software load, or later using the Service Tools. The license key is a string of 16 alphanumeric characters without any spaces. An example of a license key could be **KLEDGQYK4PXK2BKS**.

In eLicense, the keys will also have a following digit, separated by a space - **KLEDGQYK4PXK2BKS 1** – this is indicative of the number of users this license will support. All Node-locked licenses will have a 1 after the key. Floating licenses can have a 1 or any number (like 5) indicative of the number of user instances purchased for floating availability.

NOTE

This license is calculated in the GEHC eLicense web-tool, and is derived from the licenseID of the hardware – just like the Advantage Windows product. The licenseID is calculated from the MAC of eth0 by the "License" Tool interface in the **Service Tools > Initial Configuration**.

If you have the product order number (**GON**), and have access to eLicense, you can query the eLicense web interface for the license key, or create it based on the GON.

NOTE

If you do not have access to eLicense, you can proceed with the installation anyway, and enter this license along with other licenses for the advanced applications later after the software installation is complete. There will be a screen at the end of the installation indicating that the license is invalid, or has not been entered, but the software installation will complete anyway.

5.3.4 Product Network Configuration

NOTE

For the "initial" server installation, the configuration of the network consists of TWO activities:

- iLO network configuration (for physical hardware)
- Network configuration

For all subsequent software re-installations, only the network configuration needs to be performed by the GEHC FE if the service processor itself was NOT replaced or reset back to defaults.

5.3.4.1 iLO Configuration (for physical hardware)

THIS STEP IS INFORMATIONAL. IT ONLY NEEDS TO BE DONE FOR THE "INITIAL INSTALLATION - OR IF THE SERVICE PROCESSOR WAS RESET OR REPLACED.

See Chapter 7, [7.8 HP Escalation and Communication Flow on page 464](#) for details of the HP iLO Service Processor.

5.3.4.2 Server Network Configuration

CONFIGURING THE SERVER CLIENT NETWORK PORT FOR PRODUCT USE - WITH A DEDICATED STATIC IP ADDRESS – THIS STEP IS REQUIRED AFTER ALL OS SOFTWARE LOADS.

NOTE

The default out-of-the-box configuration of the OS load will set the server client network port to **DHCP** so that it will automatically pull an IP Address from the network (if the network supports DHCP).

NOTE

For a cluster of AW Servers, an additional static private IP address must be configured

- If the command prompt is not already logged into, at the login prompt - login as **root**, using the default password (unless it has been changed to something else – see [A.6 Password Change on page 484](#)).
- Command line must be used to configure the network. There are available from the Server console, as described in [A.10.3 Configuring the network card using command lines \(sys-net-conf\) on page 496](#).
- After changing a network card, new licenses will be required (generate with eLicense).

5.3.5 Configuration Restore considerations

NOTE

Be careful when using the **Restore** function.

Remember, you will be replacing system or user configuration files with the "last available backed-up versions."

The back-up tool will save a listing of the previous backup files.

So, you will have access to back-up files only as current as the most recent back-up.

And, you will be able to select from a list of older back-ups if you desire - to test with - or if you have a particular back-up file date in mind that you wish to revert to.

There are **TWO** tabs in the **Restore configuration** interface:

- *System configuration*
- *User Preferences*

In order to **restore the whole configuration after** the software **Load from Cold**, we will select the **System configuration** restoration.

This is the "home" or default tab that is displayed when the Restore tool is accessed. There are several options available for selection or use on this page.

There are **THREE** tabs in the **Source** restoration configuration file(s).

- Server
- Upload
- Last known good

Server – If you select the server radio button, this means that you have elected to restore configuration from the back-up file(s) that have been saved on the server file-system.

NOTE

This option is not appropriate for a Virtual Machine - use the Upload option instead.

- Just below the grayed-out Upload configuration button, there is a PULL-DOWN list of all the server configuration back-up files that exist on the server. These files take the form and location

of the following example - /export/backup/system/AWSBackupSyst_20080716-1544644.tar.gz

- The system will automatically save some # of these files, and over-write the oldest files, as new ones are saved / backed-up. Notice the date & time code (2008716-154466) of the file names - the most-recent back-up file will be at the bottom of the list.
- Click on the back-up file you wish to restore from the pull-down, and use the "Select" button - next to the pull-down list - to select that back-up file.

The "Select" button will fill-in the "Available configurations" pane - with the appropriate boxes checked - depending on what elements of the configuration are contained in that particular back-up file.

- Finally, click on the "Restore Selected" button to initiate the restoration.

A progress indication will display next to the "Restore selected" button, and then a GREEN successful indication - if the restore was successful. If it failed, there will be an error message indicating the failure.

In the case of a failure - notice any actionable messages in the message, and pursue the details - OR -

- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the "restart" function from the HealthPage.
- Reboot the server.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Reload the platform and/or OS software (LFC).

Upload - If you select the Upload radio button, this means that you have selected to restore configuration from back-up file(s) that have been saved in an external file location - like the OLC back-office server, a location on your PC, or a portable media.

NOTE

This option must be used in the case of an AW Server installed on a Virtual Machine.

- Click on the "Upload configuration" button. A small pop-up window (**Send files to server**) will display, presenting the ability to "Browse" to a file location, also with a "Send to AW Server" and **Cancel** button.
- Browse to the location of the configuration back-up file, select it, and then click the "Send to AW Server" button.
- Once the configuration file is sent to the AW Server, it will appear in the PULL-DOWN list - just beneath the Upload configuration button. These files take the location, and form of the following example - /var/lib/ServiceTools/upload/(\$SystemId)_backupSyst_ _2008-714-111337[1].tar.gz (where SystemId is the SystemId of the server)
- Click on the back-up file you wish to restore from the pull-down, and use the "Select" button - next to the pull-down list - to select that back-up file.
- The "Select" button will fill-in the "Available configurations" pane with the appropriate boxes checked, depending on what elements of the configuration are contained in that particular back-up file.
- Finally, click on the "Restore Selected" button to initiate the restoration.

- A progress indication will display next to the "**Restore selected**" button, and then a GREEN successful indication – if the restore was successful. If it failed, there will be an error message indicating the failure.
- In the case of a failure – notice any actionable messages in the message, and pursue the details - OR –
- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the "**restart all**" function from the HealthPage.
- Reboot the server.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Reload the platform and/or OS software (LFC).

Last known good – If you select this server radio button, it means that you have elected to restore the specific configuration from the back-up file(s) that have been saved on the server file-system which automatically include **ALL** available configurations in the back up.

The last known good configuration (**LKGC**) is not different than a normal system back up, except for the following specific differences:

It is designed to always be a complete or total system back up.

It is saved in its own specific file system location, separate from the normal system back up file

- `/export/backup/last_known_good/($SystemId)_backupSyst_20080716-154713.tar.gz` (this is an "example" file name to illustrate the naming convention)

It is meant to be a FULL system back up that can be used for system restoration to the last known good configuration after a service or failure scenario that has corrupted or deleted the current configuration.

- Just below the grayed-out Upload configuration button, there is a PULL-DOWN list of all the **LKGC** server configuration back-up files that exist on the server. These files take the form of the following example - `/export/backup/last_known_good/($SystemId)_backupSyst_20080716-154644.tar.gz`
- The system will automatically save ## of these files, and over-write the oldest files, as new ones are saved / backed-up. Notice the date & time code (2008716-154466) of the file names - the most-recent back-up file will be at the bottom of the list.
- Click on the LKGC back-up file you wish to restore from the pull-down, and use the "**Select**" button - next to the pull-down list – to select that back-up file.

The "**Select**" button will fill-in the "**Available configurations**" pane with the appropriate boxes checked - for the **LKGC** this should be all of them.

- Finally, click on the "**Restore Selected**" button to initiate the restoration.

A progress indication will display next to the "**Restore selected**" button, and then a GREEN successful indication – if the restore was successful. If it failed, there will be an error message indicating the failure.

- Perform a server **REBOOT** to be sure that all configurations get integrated.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

In the case of a failure – notice any actionable messages in the message, and pursue the details
- OR -

- Retry the restore.
- Retry the restore with a different configuration file or location.
- Perform the "**restart all**" function from the HealthPage.
- Reboot the server.

NOTICE

Before performing a shutdown or reboot, refer to [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

- Reload the platform and/or OS software (LFC).

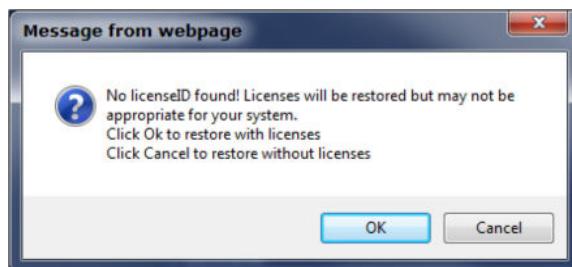
NOTE

If the system backup file does not contain the keyword "**backupSyst_**", then the upload may be successful but the back up will never appear in the restore section.

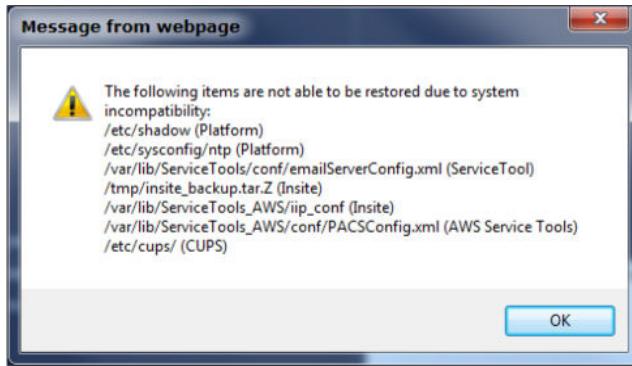
5.3.6 System configuration restore from AW Server 2.0

When restoring a backup file created on AW Server 2.0, the following should be taken into account:

- AW Server 2.0 backup files do not contain the licenseID. When restoring one of this file, a pop-up will be displayed to indicate that no licenseID was found. There are two choices:



- Click "Ok" to restore with licenses. Choose this solution if you are restoring a backup file done on the same hardware (software upgrade)
- Click "Cancel" to restore without licenses. Choose this solution if you are restoring a backup file done on a different hardware (hardware upgrade)
- AW Server 2.0 backup files contain some files that are not used anymore on AW Server 3.2. These files will not be restored:
 - the file storing the passwords is not restored.
 - the files related to insite are not restored. For version prior to AW Server 3.2 Ext. 4.2, if the system had an insite checkout previously, it is needed to do the checkout again.

**NOTE**

The following parameters are not contained in the AW Server 2.0 backup file: hospital name for filmer and recurrence backup settings. These parameters have to be restored manually.

5.3.7 User Preferences Restoration

NOTE

THIS STEP IS NOT NECESSARY, IF YOU HAVE PREVIOUSLY RESTORED THE SYSTEM CONFIGURATION, AS IT ALSO RESTORES THE USERS PREFERENCES.

There are a couple of options available for selection or use on this restoration TAB.

Source – the source of the restoration of the User Preference file(s).

Server – If you select the server radio button, this means that you have elected to restore User Preferences from the back-up file(s) that have been saved on the server file-system.

The process and work-flow is essentially the same as it is with the system configuration restoration details above – except – instead of displaying a pull-down list of the available configuration file names – like (\$SystemId)_backupUser_20080716-154644.tar.gz – **the pull-down list in the User Preference restoration tool will display a list of the USERS that preference files are saved for.**

NOTE

If the system backup file does not contain the keyword "backupUser_", then the upload may be successful but the back up will never appear in the restore section.

IMPORTANT FINAL STEP IN SYSTEM OR USER PREFERENCE RESTORE PROCESS.

There are two levels to determining if the restoration is implemented or not:

- The restored system configuration shows in the Service Tools sections – HealthPage, device data, contact data, DICOM hosts, Users, Licensing, and so on ...
- The system configuration is available in the client application when the user connects to the server. Essentially this means – does the "system" work?

There is no ONE-way to determine if the restoration was completely successful by examining any ONE thing in either of these TWO operational levels.

TO RELIABLY RESTORE THE BACKUP REBOOT THE SERVER AFTER THE RESTORE IS COMPLETE. IF YOU DO NOT, THERE IS THE POTENTIAL THAT SOME OF THE RESTORATION MAY NOT HAVE BEEN IMPLEMENTED COMPLETELY – IF AT ALL.

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

NOTICE

After performing a software reload or upgrade, ensure that all default passwords are changed to unique, complex passwords. (Note that in many hospitals, accounts are managed via EA3 however. The root account password is not within scope and thus will not be backed up). Note that if you change the service account password, you must advise the OLC.

NOTICE

After performing a software *upgrade*, you should destroy any old versions. Refer to [A.17 Secure Media Destruction Procedure on page 511](#).

5.3.8 Registration

GIB Registration

When upgrading or installing an AW Server system to a new release, do not forget to update GIB.

There is one GIB link (for US, EMEA, Asia/Pacific) for GEHC-HCS and GEHC-IT:

EGIB @ <http://gib.gehealthcare.com>

Configuration Registration

Perform Configuration Registration as described in Chapter 4, [4.9 Register Configuration on page 416](#).

NOTICE

Repeat this procedure after any intervention that changes the server's configuration, for instance installing a new application

5.4 OS and AW Server Platform software Service Pack installation

AW Server introduces the ability to install Service Packs on top of the current release. The Service Packs allow to fix critical vulnerabilities and bugs in the AW Server software and the underlying OS.

NOTE

The Service Packs functionality will be available from AW Server 3.2 Ext. 4.2.

NOTE

A Service Pack is compatible only with one specific AW Server release with specific extension number (i.e.: A Service Pack created for AW Server 3.2 Ext. 4.6 will not work on AW Server 3.2 Ext. 4.8).

NOTE

Service Packs are cumulative for one particular AW Server release. That means that one particular Service Pack will contain all the changes of the earlier Service Packs. Therefore it is enough to deploy only the latest one.

NOTE

It is **not** possible to uninstall a Service Pack.

The following workflow summarizes the installation steps to install AW Server Service Packs on top of the current release:

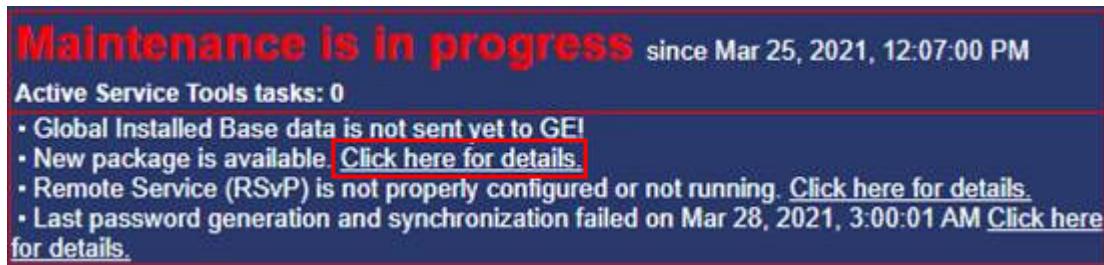
1. Put the AW Server in Maintenance Mode. Refer to [4.2.2 Start Maintenance Mode on page 389](#).

2. Backup the configuration (perform a full configuration backup). Refer to [4.4 Configuration Backup on page 394](#).
3. [5.4.1 Loading the OS and AW Server Platform software Service Pack on page 430](#)
4. [5.4.2 Installing the OS and AW Server Platform software Service Pack on page 432](#)
5. Re-apply the System Hardening. Refer to [the AW Server 3.2 Installation Manual, Job Card IST008 - Initial Configuration](#).
6. Register System configuration. Refer to [the AW Server 3.2 Installation Manual, Job Card IST013 - System Configuration Registration](#).
7. Backup the configuration (perform a full configuration backup). Refer to [4.4 Configuration Backup on page 394](#).
8. Exit the Maintenance Mode. Refer to [4.2.4 Finish Maintenance Mode on page 391](#).
9. Reboot the AW Server.
10. Check that the AW Server Service Pack information will display on the Healthpage (in **Version Information** area).

5.4.1 Loading the OS and AW Server Platform software Service Pack

For the systems connected via RSvP, if an AW Server Service Pack is available, it has been automatically loaded onto the AW Server (from the software delivery portal).

In this case, from the Service Tools, click on **Click here for details**, in front of New package is available.



Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message. Then jump to [5.4.2 Installing the OS and AW Server Platform software Service Pack on page 432](#).

Otherwise, the AW Server Service Pack has been copied to USB media through the eDelivery mechanism.

NOTE

When loading from electronic files, always refer to **AW eDelivery Service Guide 5761599-8EN** for detailed instructions.

1. Insert the AW Server Service Pack media into the Client PC or the FE laptop.
2. From the Service Tools, select **Maintenance > Version Management**.
3. Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message.
4. Click on **Upload ISO**.

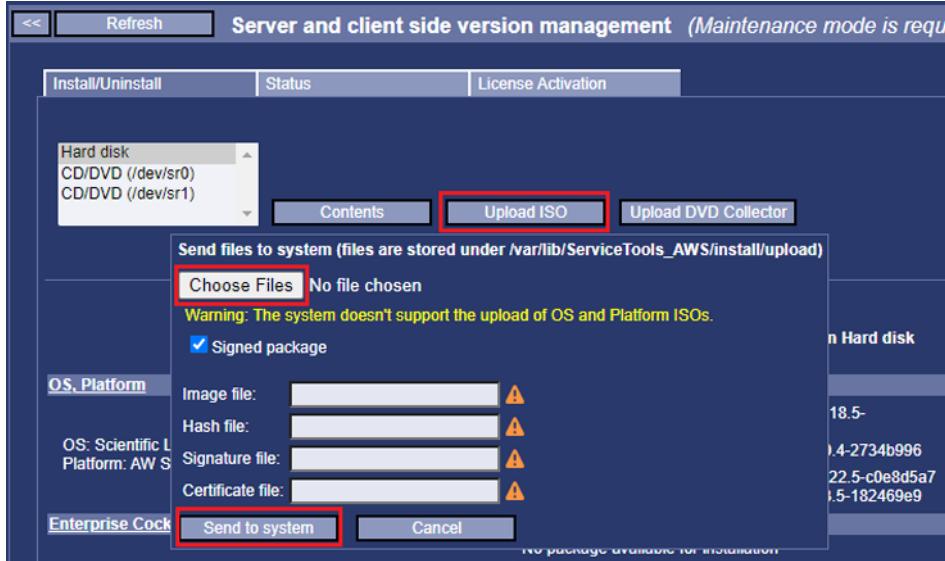
- If the Service Pack ISO file is **signed**, follow the below substeps. Otherwise, jump to next step.

NOTE

A signed ISO is composed of 4 files: the ISO itself and an hash, a signature and a certificate files which are used to check the authenticity of the ISO file.

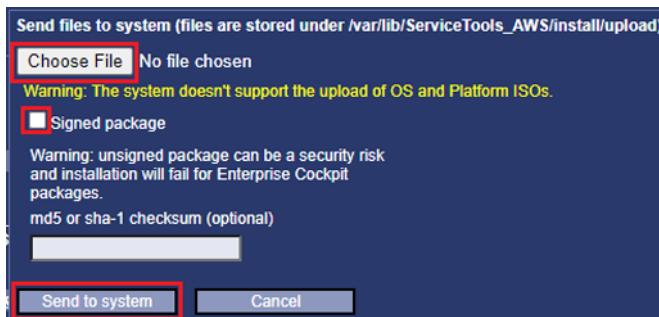
If the Secured for RMF mode is planned to be activated, only signed ISO is accepted.

- In the pop-up window click on **Choose File** and select the Service Pack ISO file as well as the hash, the signature and the certificate files, stored on the media (search for .iso, .sha256.txt, .sha256.sig and .sha256.sig.pub extensions).



- The **Image file** (Service Pack ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
- If the Service Pack ISO file is **not signed**, follow the below substeps.

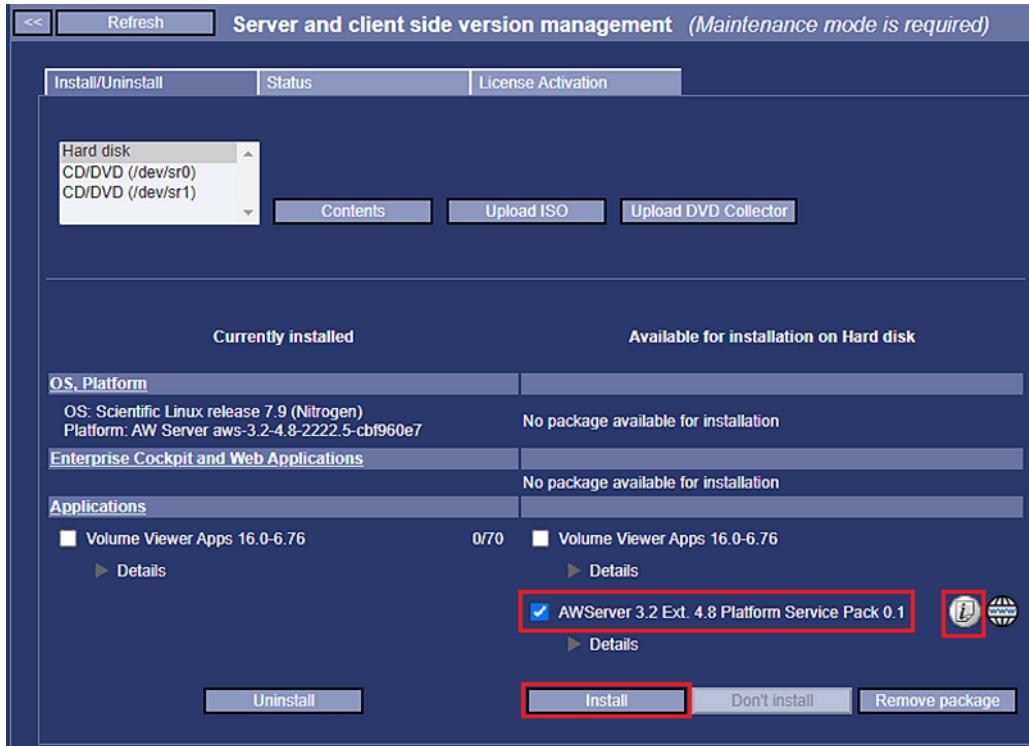
- In the pop-up window, uncheck the **Signed package** check box.
- Click on **Choose File** and select the ISO file stored on the media.



- For integrity check, copy/paste the md5 or sha-1 checksum of the ISO file, retrieved from the media, into the **md5 or sha-1 checksum (optional)** field.
- To upload the ISO file click on **Send to system**.
- When the upload is completed, acknowledge the popup that displays.
- Verify that the Service Pack appears in the Available for installation on Hard disk part of the page.
 - Remove the media from the Client PC or FE laptop.

5.4.2 Installing the OS and AW Server Platform software Service Pack

- Select the AW Server Service Pack to install and click on **Install**.



NOTE

For the systems connected via RSvP, if an AW Server Service Pack is available, it has been automatically loaded onto the AW server (from the software delivery portal), and the  icon is displayed in front of the applications name. If installation instructions are available, the  icon is also present in front of the applications name. Click on it to review the instructions.

- In the pop-up window, click on **OK** to proceed with installation.
The installation status page displays the installation steps.
When the installation is completed, acknowledge the popup that displays.
- Select the **Install/Uninstall** tab.
- Check that the AW Server Service Pack appears in the **Currently installed** part of the page.
- The AW Server Service Pack information will display on the Healthpage after a reboot as shown in the screen shot below.

Version Information	
AWS Service Pack version	aws-sp-3.2.4.8-0.1.noarch
Component Registration	1.0.4-1
AWS build date	20220607
AWS version	aws-3.2-4.8-2222.5-cbf960e7

The AW Server reboot will be done later.

NOTE

If any issue occurs during the Service Pack installation or if the system does not work as expected after the Service Pack installation, use the backup created prior to install

the Service Pack and reload the current AW Server (as for an upgrade – Load From Cold).

5.5 AW Server Client Software Upgrades

NOTE

If a reload of the AW Server software has been done in order simply to *reinstall* the same version, you can bypass this step.

If the software reload has been done in order to *upgrade* the software version, you will need to upgrade the AW Server Client software as well. Proceed with one client workstation upgrade using the procedure given below. Then notify the IT department of the hospital, so that they upgrade the other client workstations.

Do not forget to perform the Server and Client Installation Validation Tests after reinstallation. Refer to the AW Server 3.2 Installation and Service Manual, section "Server and Client Installation Validation Tests".

5.5.1 Client upgrade Procedure

You will now install the **AW Server client** software.

5.5.1.1 AW Server Client upgrade Procedure on Windows

This procedure is for AW Server Client not in seamless integration. For AW Server Client in seamless integration (Universal Viewer), see [5.5.1.2 AW Server Client for Universal Viewer upgrade Procedure on page 436](#)

For all systems on which a previous version of AW Server Client 3.2 was installed, it is necessary to upgrade to the newer version of AW Server Client. On the Windows PC, follow steps below to upgrade the AWS Client:

Uninstall the previous version of AWS Client

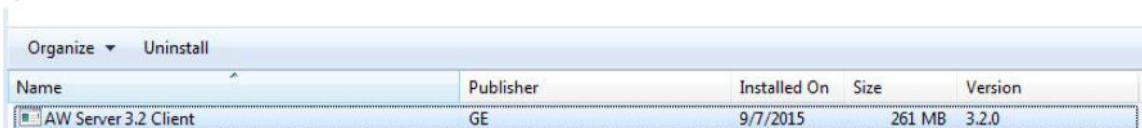
NOTE

If the AW Server Client 2.X, 3.0 or 3.1 is installed on the customer PC, it is not mandatory to uninstall it. AW Server Client 3.2 can be installed in parallel to these versions. This can be useful when accessing multiple AW Server which are running different versions. If a previous version of AW Server Client 3.2 is installed, it is mandatory to manually uninstall it before installing the newer version.

1. Open the Control Panel menu, and select **Uninstall a program** (ensure that you are viewing by Category)

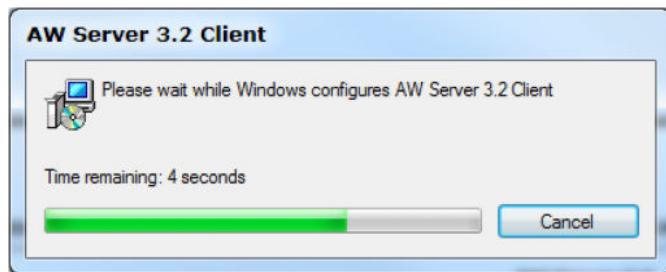


2. In the list, select AW Server 3.2 Client.
3. Click the **Uninstall** button.



Alternatively, instead of steps 1 to 3, you can perform the following: In the start menu, click on **AW Server**, then click on AW Server 3.2, then click on **Uninstall**

4. An uninstall confirmation pop-up displays. Select **Yes**.
5. A progress bar will display as follows:



- Once the pop-up closes, AW Server Client is uninstalled. You can check that it doesn't appear in the list of available programs or in the Start Menu.

Install the new AW Server Client version

- Connect to the AW Server home page, using the url http://<IP_of_AW_Server> (e.g. <http://10.12.52.45>)
- Next to Client for Windows click on **Download**. Follow the instructions of your Web browser to save the file on your local disk.

Figure 5-2 For AW Server 3.2 Ext. 4.0 and prior:

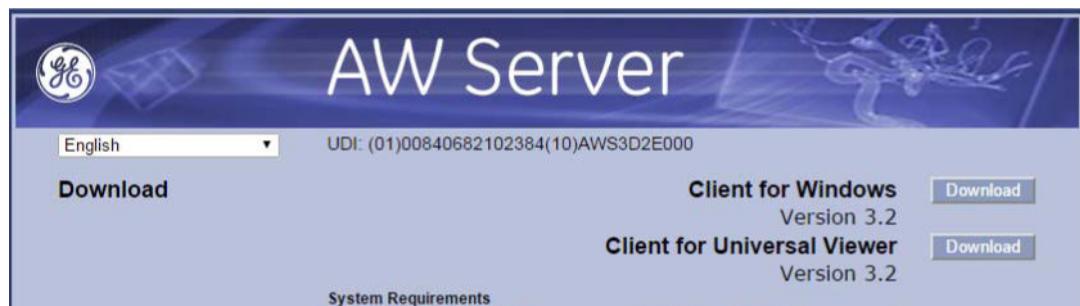


Figure 5-3 From AW Server 3.2 Ext. 4.2 with new User Interface:

AW Server 3.2 Ext. 4.2

UDI: (01)00840682102384(10)AWS03D02E4D2

English ▾

System Requirements

Processor: Intel® Core™2 Duo processor @2.33GHz or Pentium® processor 4 @3GHz minimum (or equivalent)
 Memory: 4GB minimum
 Disk drive: 500MB free space available
 Screen resolution: 1024H x 768V minimum with full color (32 bit) recommended
 Network card: 100 Mbps minimum (1000 Mbps recommended)
 Internet connection: Customer-provided IPSEC VPN, for internet/WAN operation
 Mouse: Two or three-button mouse. Two button mouse with scroll wheel suggested for best use of functions.
 Operating systems: Windows® 10 32bit and 64bit
 Certain GE consoles are also supported. See the corresponding console User Guides for further details.

Client for Windows Version 3.2 Ext. 4.2	Download
---	-----------------

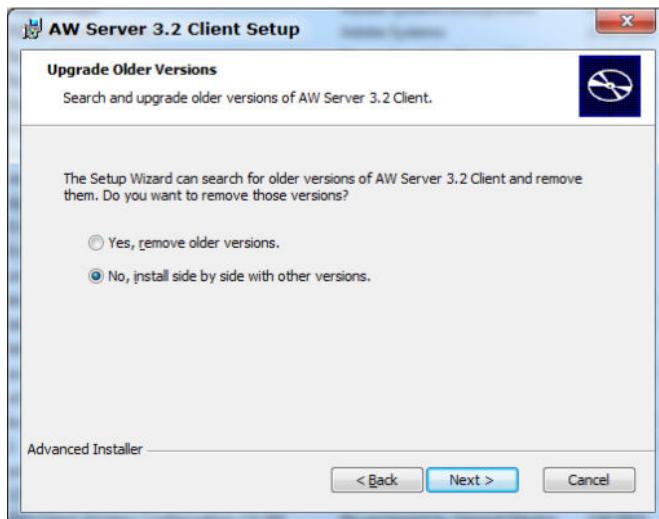
- Once the file is downloaded, open it. The AW Server Client installer starts.



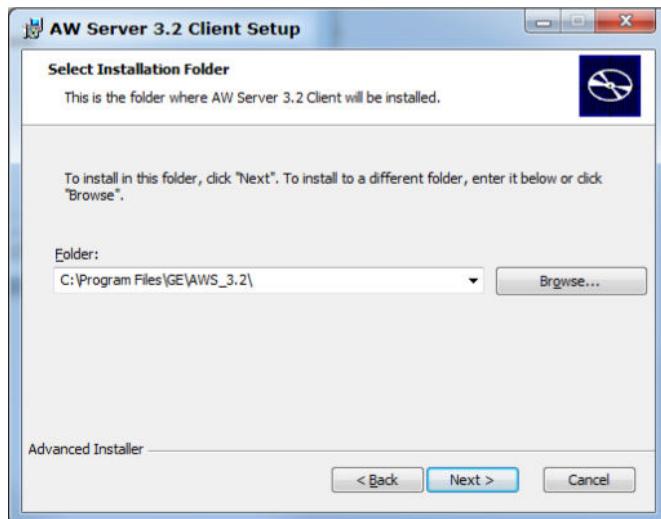
4. Select **Next**.
5. The following screen allows to remove previous version of AWS client or to keep them.

- Yes, remove older versions: if you select this option, the installer will find all previous AW Server Client install and remove them: AW Server 2.0, AW Server 3.0 and AW Server 3.1. Be aware that the uninstallation of these releases can take several minutes. **Note:** This will not remove AW Server Clients for Universal Viewer as they are stored in a different folder.
- No, install side by side with other versions (default option): if you select this option, the installer will keep all previous AW Server Client versions. Choose this option if you need to connect to AW Server running different major version.

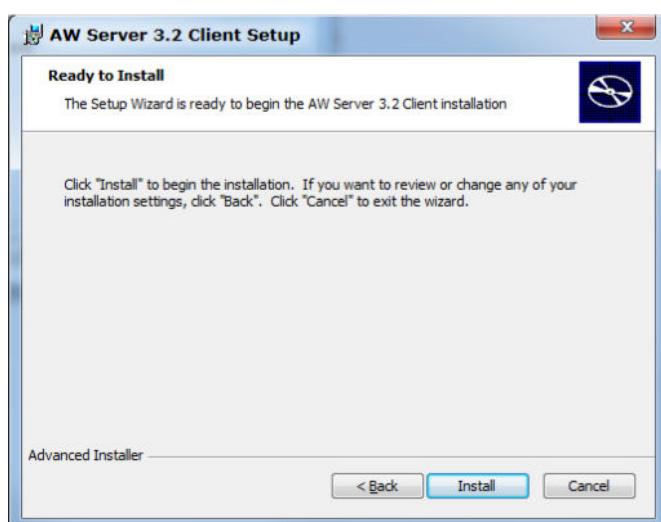
Once you have selected the appropriate option, select **Next** to continue.



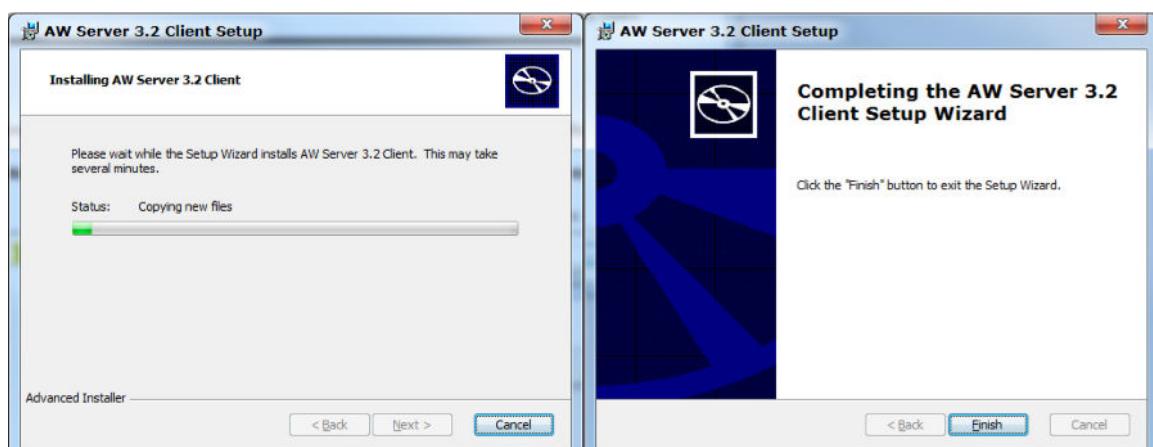
6. The following screen allows to choose the installation folder. Unless there is a specific need, keep the default value.



7. Select **Next**. On the next screen, select **Install**.



8. A progress bar will display. Once finished, select **Finish** to close the installer.



5.5.1.2 AW Server Client for Universal Viewer upgrade Procedure

To install or upgrade the AW Server Client for Universal Viewer, refer to the AW Server 3.2 Installation and Service Manual, Job Card IST014B - Seamless Client PC installation and Tests.

To check that AW Server Client was correctly installed, do the following:

- In Windows, select **Add/Remove Programs** in the Control Panel. Check if the following application is listed: AW Server 3.2 Client for Universal Viewer.

- In Windows Explorer, check that the following folder exists and contains files: C:\Program Files\Integrad.3\MIV\Solomini\3.2\solomini\. The path may be different depending on your system and disk configuration.

5.5.1.3 AW Server Client Installation Procedure on Linux

Installation of AW Server Client on Linux is not currently supported in this AW Server release at the time of release.

However, certain GE consoles may be supported.

See the corresponding console User Guides for further details.

5.5.1.4 Client Monitor screen resolution setup

By default, the Client software is setup for standard **1600x1200** pixels screen resolution monitor. Your customer may be using larger monitors for their Client PCs (2MP or 3MP monitors)

NOTICE

The 1600x1200 limitation is for performance reasons. Performance will heavily drop if these values are changed for 2MP or 3MP displays.

5.5.1.4.1 Pre-requisite

- The Network must be performing well (min 100Mbps)
- This setup must be done for each Client PC using a "non-standard" screen resolution.

5.5.1.4.2 Procedure for Windows Client PC running Windows

Use the *Windows Explorer* to edit the "solo.ini" file.. Go to C:\Program Files\GE\AWS_XX-x\solo\ (where AWS_XX-x is the AWS release)

- Make a backup copy of the "solo.ini" file: **cp solo.ini solo.ini.save <Enter>**
- Edit the **solo.ini** file, add the following lines, then save and quit the editor:

Resolution	Add these lines in "solo.ini" file
2MP monitors (1920x1200)	-DmaxNXWidth=1920 -DmaxNXHeight=1200
3MP monitors (2048x1536)	-DmaxNXWidth=2048 -DmaxNXHeight=1536

5.5.2 Server and Client Installation Validation Tests

You will now perform some basic tests to validate the AW Server system installation.

NOTE

This is a test of functionality, not relative performance. Noticeable "hangs" or delays (beyond a reasonable time) might indicate a test failure.

The **server stand-alone test** is a diagnostic test of the server only, without the network and client. It uses two tools from the AW Server Service Tools:

1. The system **HealthPage**
2. The server diagnostic test

The **client connectivity test** is a system test. It attempts to run an AW Server application from a client PC via the site's network. This tests the AW Server as a system.

NOTE

This step is not supported in seamless integration, as the AW Client is fully integrated in the Universal Viewer client.

5.5.2.1 Server Stand-Alone TEST

You will now perform the server standalone test.

This test uses the Service Tools **HealthPage** and the **Server Diagnostic Test** to determine whether the server is working properly, independent of the rest of the system.

If both parts of the Server Stand-Alone Test pass, the server is working as expected.

5.5.2.1.1 HealthPage Test

This is the first part of the Server Stand-Alone Test. The HealthPage evaluates the system hardware and platform software sub-systems.

5.5.2.1.2 Procedure

1. Connect the client PC to the site's local network for the AW Server.
2. Open a web browser (e.g., Firefox® or Internet Explorer®).
3. Enter the AW Server's IP Address in the address bar, then press **<Enter>**.

(Example of address bar IP address – <http://3.70.211.201>)

The AW Server landing page displays.

4. Click on the **Launch** button next to **Service and Administrative Tools**.

The Service Tools login page displays.

5. Login as **service**.

The Service Tools HealthPage will display as shown in the following illustration example

6. Each right-hand column on this page shows color-coded status information indicated by a **GREEN**, **YELLOW** or **RED** background. Green means that the status or value of that item is OK. Yellow means not critical, so it is considered as OK (i.e: Mount count for fsck is highlighted in Yellow if the values are close to max values) .

Red indicates a problem. A white background indicates that "status" is not applicable for that item. **Any item with a red background indicates a failure which must be investigated and fixed.**

The screenshot displays several status tables:

- Hardware Subsystem:** Shows fields like Temperature (OK), Fan Status (Not critical), Voltage (Not applicable), Power Status (Not critical), UPS Status (Not applicable), and RAID Status (OK). A red arrow points to the 'Voltage' field.
- System Configuration:** Lists various server parameters such as System ID (AWBULCLAB237), Platform version (aws-3.2-3 2-1902 5-975c1d6d), and Uptime (16 days).
- Virtual Machine:** Shows CPU (OK), Memory (RAM) (OK), Network Interface Controller (OK), and Storage (OK).
- Software Subsystem:** Lists services like Image Management Subsystem (OK), Firewall (OK), Audit Server (OK), and many others.
- Software Subsystem essential for Service Tools:** Shows services like httpd (OK), tomcat (OK), rmiregistry (OK), servicermi (OK), and awsservicermi (OK).

Annotations in red text and arrows highlight differences between physical and virtual environments:

- "For HP Servers (DL580), these fields are normally displaying in Yellow when status is OK" (referring to the 'Voltage' field in the Hardware Subsystem table).
- "With virtual AW Server, all fields shall display in green" (referring to the green background of the Virtual Machine and Software Subsystem tables).
- A note at the bottom of the Software Subsystem table states: "Restarting these services should only be performed by a qualified service or IT operative." with a "Restart" button below it.

7. Check all the following areas for problems:

The **Hardware Subsystem** area.

Click the **Sensor Details** button to display all available hardware sensor data. Verify that there are no problems.

The **System Configuration** area lists basic server parameters. The previous illustration shows normal values for the AW Server as of this writing.

However, the Registration key is invalid or has not been setup yet.

The **Software Subsystem** shows the status of various software subsystems. Investigate details of any error conditions by analyzing the corresponding error logs in the **Diagnostic - Log Viewer** tool selection.

The **Software Subsystems essential for Service Tools** displays the status of services which must be running in order for Service Tools to work.

NOTE

Hover your mouse cursor over each green or red item in System Configuration to see additional information.

NOTE

The names in parentheses after each software subsystem **service name** also appear after the **log names** in the log viewer. Use this name to select the log(s) that contain information about that particular software subsystem service. For example, for the “**Firewall**” service, the log name is “pnf”.

NOTE

The **Software Subsystem** area also has a **Restart** button. This button is **NOT** part of this procedure.

A **RED** indicator in the **Hardware Subsystem** table or on the **Sensor Details** page indicates a failure in the server hardware. (Click on the **Sensor Details** button to view the details page.)

- Not all hardware failures will cause the server to be down completely. A few examples are: Fans that are in the process of failing, disk drives that have failed-over in the RAID, and correctable memory errors. **It is IMPORTANT to catch the failures that the system can temporarily withstand, before they cause the server to go down!**
- Any hardware failure is a stand-alone test failure, and requires investigation and resolution by the hardware vendor. Contact the GEHC Online Center to dispatch the hardware vendor.
- If the system is not functioning, or is having some other issues that have caused a request for service, and the Health Page is accessible, any hardware sensor failure should be treated as the immediate cause of the system failure(s), and dispatched to the vendor for resolution before any further troubleshooting is done.

A **RED** indicator in the **Software Subsystems Status** table indicates a failure in the server software subsystem.

NOTE

Some of these failures (e.g., filmer subsystem, firewall, Secure Direct Connect, printing service) will probably not make the server fail. **But, they are still failures, and must be resolved due to their potential impact on the user.**

“Potential” resolution process flow for Software Subsystem failures:

- Investigate the corresponding software error log(s) in the **Diagnostic - Log Viewer** the service tools to attempt to understand the nature of the failure, and design appropriate action.
- The parenthetical (**name**) after the software subsystem component will also be in parenthesis after the log file name in the “**Log Viewer**”.

Examples: Software Subsystem – **Super Server (aweservice)**

Example: Log File – **Platform: AWE install log (aweservice)**

- Restart the software subsystem - **Restart**

Remember though, that restarting the software subsystem is just like rebooting the server – it will disconnect all users!

- Restarting the software can also be done from commandline:

/usr/share/ServiceTools/scripts/healthpage/restart_st.sh <Enter>

/usr/share/ServiceTools/scripts/healthpage/restart_all.sh <Enter>

(the “**Restart**” button is mapped to this script)

- Reboot of the server – **will disconnect all users.**
- Re-installation of the application software package(s).
- Load-From-Cold (OS software and system rebuild).

If ALL items in the STATUS columns for Hardware Subsystem (and Sensor Details page), Software Subsystem, and Software Subsystem essential for Service Tools are GREEN, the first stage of the stand-alone test has passed.

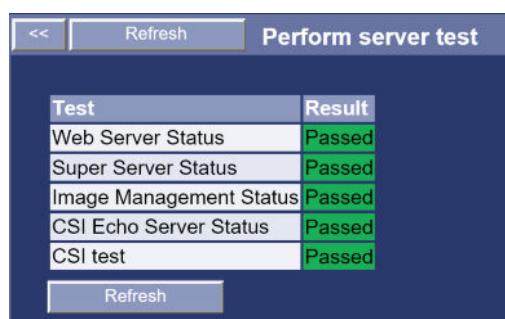
5.5.2.1.3 Server test

The second stage of the server **stand-alone test** is a diagnostic designed to test the server's advanced applications services and data.

NOTE

This test must be executed from a network PC. It will not display correctly - or at all - using the local keyboard and display via the Linux desktop ("X") environment.

1. In the Service Tools menu, click on **Diagnostic** to expand that menu. Then click the arrow next to **Test** to expand the menu.
2. Click on **Server**. The **Platform server test** interface should display as shown in the next illustration.



The screenshot shows a software interface titled "Perform server test". At the top, there are buttons for "Refresh" and "Perform server test". Below this is a table with two columns: "Test" and "Result". The table contains the following data:

Test	Result
Web Server Status	Passed
Super Server Status	Passed
Image Management Status	Passed
CSI Echo Server Status	Passed
CSI test	Passed

At the bottom of the interface is a "Refresh" button.

3. After a brief pause, the results for each test in the "Result" column should list the status of each test as "Passed" (all results should be GREEN).

NOTE

If there is a failure, use the same resolution process as with the HealthPage Software subsystem status described previously: Log Files analysis --> possible restart --> software reload, etc.

4. **If the health-page software subsystem status indications are all GREEN, and the platform server tests both pass - then the AW Server Stand-Alone Diagnostic has passed**, and the server is now ready for system/client testing.

5.5.3 Troubleshooting

If a problem occurs during the installation / upgrade of the AW Server Client, check the following.

5.5.3.1 Troubleshooting in no integration mode

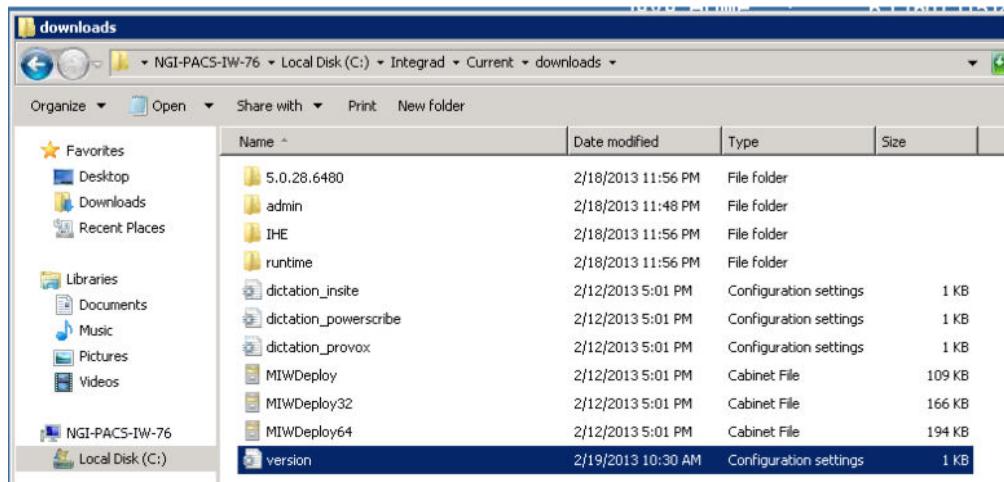
In case of issue of the AW Server Client:

- Check that you are using the correct version of AW Server Client installer. In case of doubt, display the home page of the AW Server you want to connect to, and download the AW Server Client installer again.
- Check that there is no other version of AW Server Client 3.2 installed on your system. If there are any, uninstall them, then retry the installation of the new AW Server Client 3.2 version.

5.5.3.2 Troubleshooting in Seamless integration mode

If a problem occurs during the installation / upgrade of the AW Server Client, check the following:

1. The following instructions assume that the installables for the AW Server (SoloMini) Client have already been upgraded on the Universal Viewer Server (PACS), according to the procedure described in the AW Server 3.2 Installation and Service Manual.
2. Obtain the version identifier for the upgrade release (supplied in the \client\release.txt file on the corresponding AW Server Software media. (Alternatively available from an installed AW Server with the appropriate version, via a browser connection to the following URL: http://<AW_SERVER_IP>/client/release.txt)
3. Using a text editor (such as Wordpad) open version.ini in the Integrad\Current\downloads folder.



4. Check the listed version under [SOLOMINI], and if necessary edit it to match that of the upgrade, for example VERSION=3.2-1.0.
5. Check that a folder exists in C:\Integrad\Current\downloads\runtime\Solomini with the name of the upgrade version (for example VERSION=3.2-1.0).
6. Check that the folder found in the previous step contains the downloadable msi file for the upgrade, for example: SolominiInstaller.msi
7. On the client workstation, change the Admin rights of the following folder: c:\Program Files (x86)\Integrad.3\MIV\.
 - a. Right-click on the folder in Windows Explorer.
 - b. Select **Properties > Security > Edit > Add**.
 - c. On the Groups page, enter **Everyone** in the text box.
 - d. Click **OK**.
 - e. Check **Full Control**.
 - f. Click **OK**.

NOTE

When a user tries to open an exam using an AW Server application, it checks the local version.ini file and detects that a new version of the AW server client is available on the server. The workstation is automatically upgraded from the corresponding folder on the server.

Chapter 6 Planned Maintenance (PM)

6.1 Job Card SV001 - Planned Maintenance (PM)

The server hardware does not have a PM requirement from the Vendor.

However, the server hardware has several fail-over components that are configured to allow the server to keep functioning if one of them should fail.

Both the server and direct attached storage have redundant power supplies, and disk drive RAID configurations that allow operation should one of the drives fail. The server also has multiple fans and temperature sensors that can alert service to a failure before it becomes critical.

The software on the server has several ways in which it detects these components and sensors. GEHC is not currently able to systematically monitor the sensors to provide pro-active alerts.

In order to take advantage of the fail-over capabilities of the product, and potentially resolve failure issues before they cause the server to be down – it is advisable to periodically check the software sensors on the product. If any faults are observed, requests for service should be through the GEHC service request process.

PM is necessary to pro-actively detect software related issues, such as expiration of digital certificate, limited free disk space...

PM applies to both physical and virtual AW Servers.

6.1.1 Recommended PM Schedule

Recommended PM (local PM or remote PM depending on the system accessibility) is as follows:

- **Physical server: 1 PM per year** - HealthPage, disk errors and sensors checks - unless specific monitoring is in place.
- **Virtual server: 1 PM per year.**

NOTE

EDS does not require PM for systems monitored via Centricity OnWatch.

NOTE

The frequency of PMs could be changed later if too frequent or not frequent enough.

6.1.2 PM Access

- Remotely via the InSite/RSvP connection (or EDS equivalent remote access).
- Locally via the server keyboard – display – mouse.

6.1.3 PM Time

- The PM should be scheduled for no more than 1 hour (1/2 hour typical).

6.1.4 PM Tasks

The main purpose of PM is to check the software sensors - primarily for any hardware faults, but also for software errors.

NOTE

Some of the elements in the HealthPage Server Configuration Table are STATUS indicators – like the **DICOM Queue Status** – and while they might merit attention, they are not hardware or system failures requiring separate service dispatch creation. Investigate them as PM analysis actions, and only create service follow-up dispatches if the investigation leads to discovery of a system fault condition.

6.1.4.1 Check Version Management

If the Service Tools notified you that new software packages are available, go to "Maintenance" > "Version Management" menu and install or refuse available updates.

6.1.4.2 Check the Healthpage

These tests are **NON- INVASIVE**, and can be performed at anytime. However, corrective action may require a **RESTART**, **REBOOT**, or entering **Maintenance Mode – which will be invasive to clinical use**.

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

Remotely connect to the AW Server and examine the Healthpage. Check the following items in the HealthPage:

- Hardware Subsystems or Virtual Machines section shows no red statuses.
- System Configuration status shows no red statuses for:
 - Disk space.
 - Image partition mount count and Image partition next file system check date values.
 - Certificate expiration date.
- Software Subsystem status shows no red statuses.
- Software Subsystems essential for Service Tools status shows no red statuses.
- Software Subsystem status, Firewall (pnf) display status if "OK". If not, you must turn it On and make sure that the connectivity to the AW Server is maintained.

6.1.4.3 Checking ClamAV® status and logs

1. In Service Tools, on the HealthPage, check the **Clam AV Antivirus Software** status.
If infected files are detected, it appears in red.
2. At a minimum, check the log files according to the Planned Maintenance schedule.
ClamAV® log files are located in `/export/home/sdc/logfiles`.

A scan output consists of messages concerning the latest ClamAV®, the list of files scanned and a summary.

NOTE

The message **This version of the ClamAV engine is outdated** is normally not very serious. The AW Server OS includes "a" version of ClamAV®. New versions may be released between OS releases, and thus the installed version of ClamAV® may not be the latest available. If it becomes necessary to update to the most current ClamAV®, it is the user's responsibility to access the website listed in the document <http://www.clamav.net/doc/cvd.html> and follow the update process.

Check the Infected files line in the summary. For example:

```
----- SCAN SUMMARY -----
Known viruses: 824560
Engine version: 0.96
Scanned directories: 1
Scanned files: 55
Infected files: 0
Data scanned: 1.96 MB
```

6.1.4.4 Checking McAfee status and logs

On AWS3.2 Ext. 4.8, in Secured for RMF mode, AW Server replaces ClamAV® Antivirus Software with McAfee. In this case do the following checks during PM:

1. In Service Tools, on the HealthPage, check the McAfee Antivirus Software status is **Activated**. On AWS3.2 Ext. 4.8 Secured for RMF mode, the Antivirus must be activated to have RMF compliancy.
2. Check if the McAfee virus database abd engine is up to date and update them if AW Server does not have the latest version. Refer to the *AW Server 3.2 Installation Manual*, section *McAfee Virus Database and engine update check*.
3. Check the McAfee logs either in the Hospital's central syslog server or in the local McAfee log files. Refer to [3.18 Log patterns for log analysis in RMF environments on page 379](#).
4. Apart from sending the log to the rsyslog server, if McAfee antivirus detects a threat it will put the impacted file into quarantine. Check the Scan result in **Service Tools > Maintenance > Antivirus page > Antivirus Scan Tab > Recent On-Access scan results** section. See example screenshot in case the Antivirus software has found a suspicious file:

Recent On-Access scan results							
File name	File size	File size	Time	Process name	Username	Profile type	
/export/home1/sdc_image_pool/eicar	70	EICAR Virus Type	1656663757			1	

6.1.4.5 Verify RMF compliancy

Perform this check **only** for AW Servers with Secured for RMF mode activated.

AW Server with Secured for RMF mode activated can lose RMF compliancy if configuration changes were not done properly. Check the compliancy by running the `dod_verifier` script in a terminal.

Refer to the *AW Server 3.2 Installation Manual*, section *Changing AW Server configuration in Secured for RMF mode* for more details.

6.1.4.6 Password change

Ensure that the default password have been changed to customized passwords.

Otherwise, follow instructions to change the passwords. Inform all stakeholders of password changes.

Refer to Job Card IST006 - Changing the Passwords in the *AW Server 3.2 Installation Manual* for more details.

6.1.4.7 Configuration backup

Create a backup of the system configuration on the AW Server, and on your PC, by following instructions in the *AW Server 3.2 Installation Manual*, Job Card IST016 - System Handover to Customer.

6.1.4.8 Check the Scalability page (for cluster only)

If the AW Server is part of a cluster, check the status of the cluster as follows:

- Remotely connect to the AW Server Service Tools.
- Go to **Initial Configuration > Scalability** page.
- Check that the page displays no error for AW Server nodes in the cluster as well as for HAPS nodes.

If any error is found, refer to Job Card IST012 - Virtual Servers Cluster Configuration in the *AW Server 3.2 Installation Manual* for more details.

6.1.4.9 Configuration Registration

Register the latest configuration to AWCCT Website and ensure that a Registration key is installed. Refer to Job Card IST013 - System Configuration Registration in the *AW Server 3.2 Installation Manual* for details.

6.1.5 PM Completion

If tests were successful, enter the following data into your service record:

- System ID
- System Site Name
- Date and Time
- Your Name
- Comments: “*AW Server PM tasks completed successfully - the server status is confirmed for continued normal operation.*”

If faults or critical errors, enter the following data into your service record:

- System ID
- System Site Name
- Date and Time
- Your Name
- Comments: “*AW Server PM failed the following task(s):*”
- *Details....*
- *Enter the separate dispatch number created to address the discovered failure(s).*”

6.1.6 Planned Maintenance tasks summary

Below is a summary of tasks to be performed during Planned Maintenance. This summary is for information only and must not be used as a checklist for the Planned Maintenance.

Instead, use the Digital Service Form *AW Server 3.2 Planned Maintenance Checklist* available online on SIMS Content Viewer.

All servers (High tier / Low tier)

- HealthPage - HW and VM status checked.
- HealthPage System configuration status - Disk space does not display in RED.
- HealthPage System configuration status - Image partition mount count and Image partition next file system check date values do not reach or exceed expected values. The IT Admin of the site shall be warned that Filesystem check shall be launched automatically at subsequent reboot.
- HealthPage System configuration status - Certificate expiration date shows no error. Otherwise, it is needed to renew the certificate.
- HealthPage - Software Subsystem status checked.
- Healthpage - Software Subsystems essential for Service Tools section shows no red statuses.
- System password changed.
- Stakeholders informed of password changes.
- Configuration backup saved to server and FE or client PC.
- Configuration Registration - latest configuration has been registered on AWCCT Website and a Registration key is installed on the AW Server.
- For cluster only Scalability page has been checked and no error are displayed.

Chapter 7 FRU, Break-Fix and Disassembly / Reassembly Procedures

7.1 Overview

The following information is true at the writing of this document, and for general release of the AW Server. Subsequent updates of this data may occur without this document getting updated at the same time, or at all. Updated part numbers will be setup to automatically replace their equivalent out-of-date counterparts.

The AW Server program is establishing requirements for off-the-shelf OS and hardware. These will be delivered as part of the AW Server turnkey package for customer convenience.

- OS and hardware are not part of the AW Server medical device claims.
- OS and hardware are ordered out of catalog from respective vendors. No modifications are required for these items to support the AW Server application.
- **Sun Hardware is not supported anymore** in AW Server 3.2.

Table 7-1 Responsibility for servers installation and service

Server	Installation	Service
HPE ProLiant DL360 Gen10 Server Low Tier	GEHC	HPE
HPE ProLiant DL360 Gen9 Server Low Tier	GEHC	GEHC
HPE ProLiant ML350p Gen8 Server	GEHC	GEHC
HP ProLiant ML350 G6 Server	GEHC	GEHC
HPE ProLiant DL360 Gen10 Server High Tier	GEHC	HPE
HPE ProLiant DL360 Gen9 Server High Tier	GEHC	HPE
HPE ProLiant DL560 Gen8 Server	GEHC	HPE
HPE ProLiant DL580 G7 Server	GEHC	HPE

7.2 FRUs (Field Replaceable Units)

The Software FRUs are available in the AW Server 3.2 *Read Me First*. The full list of Hardware FRUs are available in the AW Server Hardware FRUs list Service Note (SNAW3022)

NOTICE

When ordering a Software FRU, always check that the software version of the FRU is the same as the software version that was previously installed on the system. If the FRU contains a newer software version.

7.3 Break-Fix Processes

7.3.1 Responsibility of the hardware break/fix process

AW Server hardware		Responsible
High Tier	HPE ProLiant DL360 Gen10 Server	Vendor
	HPE ProLiant DL360 Gen9 Server	Vendor
	HPE ProLiant DL560 Gen8 Server	Vendor
	HPE ProLiant DL580 G7 Server	Vendor
Low Tier	HPE ProLiant DL360 Gen10 Server	Vendor
	HPE ProLiant DL360 Gen9 Server	GEHC FE
	HPE ProLiant ML350p Gen8 Server	GEHC FE

7.3.2 Hardware Vendor Service Support Model

NOTE

Vendor Service support Model in not applicable in virtualized mode

For the Low Tier servers, the following support model is used:

- **Break/Fix in warranty & out of warranty:** GEHC HCS (or EDS) will manage Break/Fix: in warranty and out of warranty: To ensure this model, GEHC has identified a set of FRUs that are stored in GPRS Service data warehouse. In case, the whole server is out of order, a high FRU server is available to replace the whole unit

For the High Tier servers, the following Vendor support model is used:

- **Break/Fix in warranty:** Warranty uplift will be purchased (included in ICV (server, DAS Disk Array Storage, UPS Uninterruptible Power Supply, Peripherals) to include 4 hours, 24/7 parts and on-site service. Warranty duration is 3 years. Service business is responsible for uplift renewals post year 3 for contract customers.
- **Break/Fix out of warranty:** You must contact GE Service support to renew HP warranty contract.

7.3.3 Service Support Procedures

Reactive service procedures shall be performed as described below:

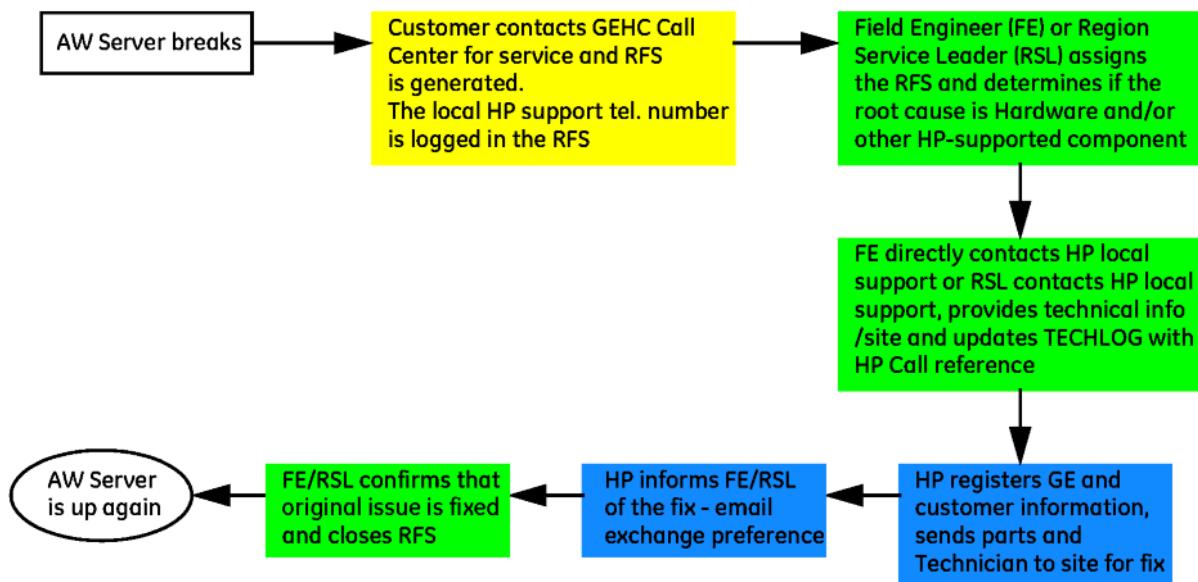
- All service calls initially placed to GEHC HCS (or EDS) FE / OLC or Field Service Engineer (FE).
- GEHC HCS (or EDS) FE / OLC perform remote preliminary triage, and if possible, resolution.
- If necessary, GEHC HCS (or EDS) OLC to split RFS (Request For Service) to the Field. For AW Server High Tier, OLC initiates vendor dispatch in case of Hardware failure.
- There is an escalation path from the GEHC IT ROC to the AW Engineering team or HCS advanced support team, for issues the EDS support team can't handle.
- Further guidance on escalation policies and routes is available at the appropriate regional Services sites.

7.3.4 HP DL580 / HP DL560 / HP DL360 Hardware - Break-Fix Process

The hardware break — fix model uses a blended vendor/GEHC model. However, when it is determined that there is a **HARDWARE** failure in the **SERVER** or any of the server's accessories, the hardware vendor is contracted through GEHC to diagnose and resolve the hardware issue.

When a problem is reported from a field site, a root cause analysis is applied and results in triage of the problem towards the appropriate resolution path.

HP Hardware Break-Fix Call Process (DL580 / DL560 High Tier Server / DL360 G9 High tier / DL360 G10 High Tier and Low Tier)



NOTE

For IT, RFS is replaced by ROC.

When you have identified or suspect a **hardware** issue, please follow use generic procedure below in order to properly involve the HP Service team (some regional differences may apply):

- Identify the Serial Numbers of the Server, DAS, UPS, Ethernet switch (as applicable).
- Note the time and date when the problem was encountered.
- Get a problem description from the end user/customer.
- Open the Terminal tool and run the `sosreport` command. This command is included in the Linux OS and will build a tar file with the system information that is used by Linux support engineers, in order to diagnose problems. The output log file is created in `/var/log` directory.
- Following the hardware issue detected (disk, fan, power supply, controller), run the appropriate command.
- Call the HP Support Center and plan a visit to the customer site, with the FP Support Center.

7.3.5 HP ML350 G6 / ML350p G8 / DL360 G9 Low Tier Hardware - Break-Fix Process

The hardware break-fix model is the **full responsibility of GEHC** for the HP server. When it is determined that there is a **HARDWARE** failure in the **SERVER** or any of the server's accessories, the hardware FRUs can be ordered from the GEHC warehouse to resolve the hardware issue.

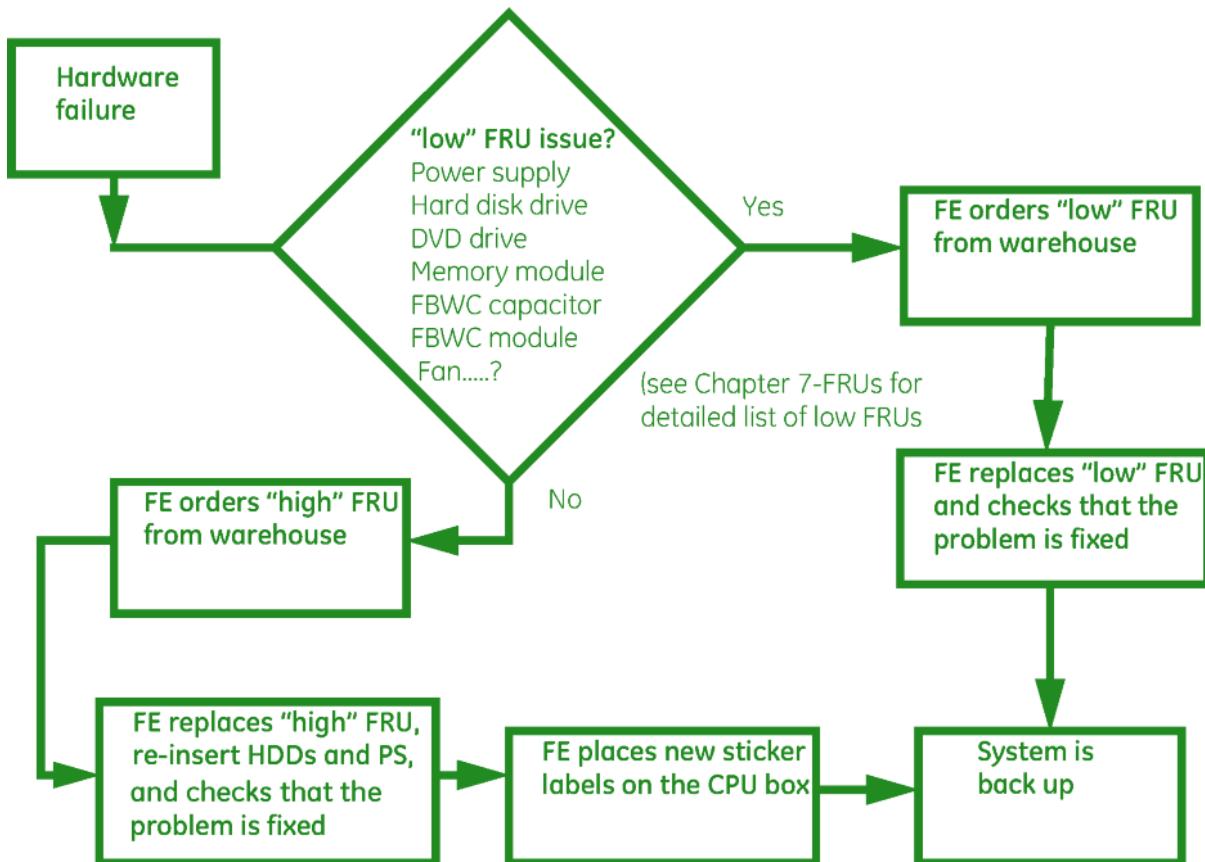
(See [3.9.6 HPE ProLiant ML350p Gen8 Server troubleshooting tips on page 320](#)).

The HP hardware FRUs and the Disassembly/Reassembly procedures are described later in this chapter. Both "low level" FRUs (Hard disks, memory modules, etc.) and "high level" FRU (ML 350 CPU box) are available.

NOTICE

The “high level” FRU (CPU box) is delivered **without hard disks**. You must use the hard disks of the defective box or order the hard disks separately.

Figure 7-1 HARDWARE BREAK/FIX FLOW OVERVIEW, HP HARDWARE.



7.3.5.1 FRU Labeling Kit

In case of a **chassis** replacement (in which labeling is lost), a new metallic regulatory labeling is applicable to AW Server Hardware. As such, a FRU Labeling Kit is required to cover the labeling of the hardware. This kit is created as a FRU that shall be ordered upon High FRU replacement for adequate labeling.

NOTE

This Labeling Kit is applicable to all hardwares running a registered AW Server platform.

NOTICE

This Labeling Kit contains regulatory labeling required in certain countries. For up-to-date applicability rules, refer to the local regulation and Read Me First document inside the kit (5802299-3 or up).

7.4 HPE ProLiant DL360 Gen10 Server Low Tier Hardware Disassembly/Reassembly Procedures

Servicing the HPE ProLiant DL360 Gen10 Server Low Tier Hardware is under the full responsibility of the vendor. This section is provided for reference.

Procedures are the same as those for the HPE ProLiant DL360 Gen10 Server High Tier. Follow procedures in sections:

- [7.7 High Tier Servers Hardware Disassembly/Reassembly Procedures on page 462](#) (and subsections),
- [7.5.3.2 SAS HDD on page 453](#),
- [7.5.3.3 Power Supply on page 453](#).

7.5 HPE ProLiant DL360 Gen9 Server Low Tier Hardware Disassembly/Reassembly Procedures

Servicing the HP HPE ProLiant DL360 Gen9 Server Low Tier Hardware is under the responsibility of GEHC service.

NOTE

Servicing the HP HPE ProLiant DL360 Gen9 Server High Tier Hardware is under the responsibility of the vendor. This section is not applicable and provided for reference only.

Refer to [7.8 HP Escalation and Communication Flow on page 464](#) for contact details.

NOTICE

When calling the HP support center for replacement of a defective **UPS or KVM**, prepare the Serial number of the HP DL360 server, as the serial number of these components are not tracked by HP, and specify that **you request on-site assistance** for the replacement. Otherwise, the defective part may be sent to the site without HP Engineers on-site support.

NOTE

The Network Switch has a standard warranty.

7.5.1 Electrical Precautions of the HPE ProLiant DL360 Gen9 Server Low Tier

CAUTION



No LOTO procedure as such is applicable to the HPE ProLiant DL360 Gen9 Server as the internal voltages of the server correspond to those of a standard "plug and cord" workstation with no residual energy. Service procedures are thus deemed to carry negligible risk. However, FEs must begin any service intervention that requires opening the HPE ProLiant DL360 Gen9 Server case with the following procedure, referring to instructions in section [3.1 Overview on page 124](#).

1. Perform a server shutdown procedure, preferably from within the AW software, OR by depressing the On/Off switch on the front panel.
2. Disconnect the two power cords from the electrical outlet and then from the server.
3. Remove the two power cords and any spare power cords from the vicinity of the server, storing them in a safe place.

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of other important precautions to take.

7.5.2 De-racking the HPE ProLiant DL360 Gen9 Server

CAUTION



The HPE ProLiant DL360 Gen9 Server CPU box weighs approximately 15 kg (30 pounds). Comply with the HP safety recommendations provided in the section "Remove the server from the rack" or equivalent in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.

7.5.3 Replacing HPE ProLiant DL360 Gen9 Server Low Tier Components

Comply with the component-specific procedure provided in the chapter "Removal and replacement procedures" or equivalent in the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008.

7.5.3.1 HPE ProLiant DL360 Gen9 Server Low Tier high FRU swap

- Refer to AW Server 3.2 Hardware Installation Manual, Job Card IST005 - HPE ProLiant DL360 Gen9 Server Installation Steps.
- Also refer to the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008:
 - Section "Extend and remove the server from the rack" (Disconnect cables)
 - Section "Access panel" (if applicable).

7.5.3.2 SAS HDD

HDDs are "hot-swappable" units. They shall be replaced with the system up and running.

7.5.3.3 Power Supply

- Power supplies are "hot-swappable" units. They can be replaced one at a time with the system up and running. Disconnect the power cable from the power supply and extract the unit.

7.5.3.4 16GB DDR4 2400 MHz DIMM

- Refer to the HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008, section "DIMMs".

7.5.3.5 Removing the internal DVD-RW drive

1. Disconnect cables.
2. Extend and remove the server from the rack.

Refer to HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 sections "Extend the server from the rack" and "Remove the server from the rack".

3. Remove the access panel.
Refer to HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 section "Access panel".
4. Disconnect the cable from the DVD-RW unit.
5. Use the Torx screw driver to unscrew.

6. Extract the drive from the front of the server.



- 1- Disconnect the cable
- 2- Unscrew the Torx screw
- 3- Extract the DVD-RW drive

7.5.3.6 Removing the fan module

1. Disconnect cables (optional, fan modules are hot-plug devices).
2. Extend and remove the server from the rack.
Refer to HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 sections "Extend the server from the rack" and "Remove the server from the rack".
3. Remove the access panel.
Refer to HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 section "Access panel".
4. Extract the fan module.
Refer to HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008 section "Fan module".

7.5.3.7 System battery

- Refer to HP DL360 G9 server Service and Maintenance Guide (Part No. 5771768-1EN) - System battery at page 62

7.5.4 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the 70-persistent-net.rules file with the the following command:
/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>
3. Reboot the server.
reboot <Enter>

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.

- b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

7.6 HPE ProLiant ML350p Gen8 Server / HP ProLiant ML350 G6 Server Disassembly/Reassembly Procedures

The following section gives directions to disassemble and reassemble the HPE ProLiant ML350p Gen8 Server / HP ProLiant ML350 G6 Server hardware FRUs (Field Replaceable Units).

- For the HPE ProLiant ML350p Gen8 Server, refer to HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009 and follow instructions of section "Removal and Replacement procedures".
- For the HP ProLiant ML350 G6 Server, refer to HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 and follow instructions of section "Removal and Replacement procedures".

7.6.1 LOTO Procedure for HPE ProLiant ML350p Gen8 Server / HP ProLiant ML350 G6 Server

CAUTION



Field Engineers must always adhere to the Lock Out Tag Out (LOTO) procedure when installing or servicing an HP Low Tier server. (Normally GEHC FEs are only responsible for servicing the Low Tier server; other server models are the responsibility of engineers from the respective hardware vendor).

MODE:	Imaging									
EQUIPMENT:	HPE ProLiant ML350p Gen8 Server ; HP ProLiant ML350 G6 Server									
Premises:	Customer owned locations or facilities									
SUBSYSTEM:	None									
ACTIVITY:	Installation, Planned Maintenance, Corrective Maintenance									
Equipment Specific LOTO Procedures										
Steps are to be completed in the order listed below										
Label /Tag Description	Energy Source	Magnitude	Location	Procedure for Lockout & Energy Release	Zero Energy Tryout, Verification, & Testing					

Electrical Wall Outlet	Electrical	110 / 230 VAC depending on region	Various	<p>Carry out server shutdown procedure, preferably from within the AW software, OR by depressing the On/Off switch on the front panel.</p> <p>Disconnect the 2 power cords from the electrical outlet and then from the server.</p> <p>Remove the 2 power cords and any spare power cords from the vicinity of the server.</p> <p>Apply any protective devices mandated by local EHS legislation (LOTO power socket locks, tags, adaptors).</p>	<p>Verify/ Test Equipment to assure power source has been removed by depressing On/Off Switch on the server front panel.</p>
Equipment Power Supply	Electrical	110V // 230 VAC depending on region	Within System Power Supplies	Wait 5 minutes after Power down to allow for discharge of any capacitors in the Powers Supplies	Check Power Supplies outputs using multi-meter for Zero Power status.

GEHC Field Service General LOTO Instructions**Shut Down Steps & Return to Service Summary**

The following section provides a Business Level Summary of the Key Steps for conducting a LOTO (Lockout Tagout).

Step 1:	PREPARE FOR SHUTDOWN: <ul style="list-style-type: none">- Acquire LOTO training and any related training mandated by local EHS legislation.- Understand the applicable procedures. Determine associated equipment.- Acquire any protective materials (i.e. socket locks, tags, lock adapters).- Assess consequences of shutdown. Notify all affected persons.
Step 2:	NOTIFICATION OF PERSONNEL: <ul style="list-style-type: none">- Personnel who may be affected shall be notified prior to the application and after the removal of power cords, lockout devices or tagout devices.- Personnel may include workstation operators, clinical users, technicians, engineers or area managers.
Step 3:	SHUTDOWN: <ul style="list-style-type: none">- Carry out server shutdown procedure, preferably from within the AW software, OR by depressing the On/Off switch on the server front panel.
Step 4:	ENERGY ISOLATION: <ul style="list-style-type: none">- Disconnect the power cord from the electrical outlet and then from the server.- Disconnect peripheral device cables from the server.- Remove the power cords and any spare power cords from the vicinity of the server.
Step 5:	LOCKOUT TAGOUT (If mandated by local EHS legislation): <ul style="list-style-type: none">- Attach LOTO Red Lock & filled out Red Tag (or local equivalent devices) on each point of disconnect, shut off, blank & vent as appropriate. Verify that all above is complete.
Step 6:	CONTROL STORED ENERGY: <ul style="list-style-type: none">- Assure that all stored potentially hazardous energy has been relieved, dissipated, restrained, drained or otherwise controlled (i.e. electrical capacitors) by waiting at least five minutes between power-down and opening the server case.

Step 7:	<p>VERIFY ISOLATION:</p> <ul style="list-style-type: none"> - Extremely important! Do not assume the posted shutdown procedure is accurate – Report any inaccuracies immediately to your EHS Rep. - Verify that the equipment is fully LOTO-compliant and that all energy is zero. - Zero energy tests shall include: <ol style="list-style-type: none"> 1) Attempt to operate the equipment, by the On/Off switch; 2) Check Power Supplies outputs using a multi-meter for Zero Power status.. <p>NOTE</p> <p>NEVER leave the server unattended with the case open. If you must leave the server during servicing, resecure the case. When you return to the server, check that the power cords have not been reconnected, before opening the case. If necessary, recommence this procedure from Step 3.</p>
Step 8:	<p>RETURN TO SERVICE:</p> <ul style="list-style-type: none"> - Assure that maintenance schedule has been successfully completed and any faulty FRUs replaced. - Assure that the server case and vicinity are clear of tools - Assure that all internal parts, covers and side panels have been securely reattached/reconnected. - Reconnect peripheral device cables to the workstation. - Reconnect the power cords to the workstation and then electrical outlet. - Notify affected persons that energy is to be restored. - Removes any tags and lockout devices from power sockets. - Reboot the server and assure that the equipment is functioning safely & properly.

NOTICE

All defective parts must be returned with no delay. **Parts which are not returned will be charged to the region.**

The first two Field Replaceable Units (Power supplies and Hard disk drives) are "hot-plug devices". It means that it is not necessary to power down the server to replace them.

7.6.2 Replacing the "hot-plug" power supplies

- Disconnect the power cable from the power outlet, then from the defective HP ProLiant ML350 G6 Server / HPE ProLiant ML350p Gen8 Server power supply. You do not need to shutdown the server.
- Extract the HP ProLiant ML350 G6 Server / HPE ProLiant ML350p Gen8 Server power supply (refer to section "Hot-plug power supply" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Power supply module" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009).
- Insert the new power supply and reconnect the power cable.

7.6.3 Replacing the "hot-plug" hard disk(s)

- Extract the defective hard disk drive from its slot (refer to section "SAS/SATA hard drive" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Drive" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009).
You do not need to shutdown the server.
- Insert the new Hard disk drive.
- Make sure it is properly detected (front LEDs are flashing while the disk is reconstructed).

7.6.4 Powering down the server

- To replace any of the Field Replaceable Units, you must power down the server and disconnect it from the mains power. Refer to section "Power down the server" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Power down the server" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.5 Opening the side cover

NOTICE

The boards and disk drives contain electronic components that are extremely sensitive to static electricity. Do not touch the components themselves or any metal parts. Carefully observe electrostatic discharge precautions when servicing inside the unit. Use a grounding wrist wrap and/or antistatic carpet when handling the drive assemblies, boards or cards.

CAUTION



To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

- Open the front bezel and remove it. Refer to section "Front bezel" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Remove the security bezel" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.
- Open the side cover. Refer to section "Rack bezel" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Remove the rack bezel" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.6 Replacing the DVD drive

Refer to section "Customer self repair" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Customer self repair" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.7 Replacing the air flow baffles

Refer to sections "Large redundant fan air baffle" and "DIMM baffle" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or sections "Air baffle" and "PCI air baffles" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.8 Replacing a cooling fan

Refer to section "Fan" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Fan" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.9 Replacing the DIMM memory modules

- Refer to section "DIMM" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "DIMMs" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.
- Question: One of my memory modules is broken, which FRU should I order?

- Answer: Follow the steps below:
 - Determine the hardware model of your Low-Tier server: HP ProLiant ML350 G6 Server or HPE ProLiant ML350p Gen8 Server. This can be checked in Healthpage **Machine type** field.
 - On the memory module, read the **label** indicating its capacity: 2GB, 4GB, 8GB.
 - Refer to [7.2 FRUs \(Field Replaceable Units\) on page 448](#) and identify the corresponding FRU Part Number.
- Question: I am swapping my Low-Tier HP ProLiant ML350 G6 Server with the High-Level FRU of HP ProLiant ML350 G6 Server, which memory modules should I keep, which memory modules should I return?
- Answer: You should keep the 4GB or 8GB memory modules. You should return the 2GB memory modules. Always ensure that the ML350 G6 has 24GB (6×4GB) or 64GB (8×8GB) memory configuration at the end of the FRU swap procedure. 12GB (6×2GB) is not a valid memory configuration for HP ProLiant ML350 G6 Server on AW Server 3.2 or higher.

7.6.10 Replacing the RAID Flash Backed Write Cache module(s)

Refer to section "Flash-backed write cache module" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "Cache module" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.11 Replacing the Real time clock lithium coin battery

System Real Time Clock (RTC) battery, CR2032 - 3V Lithium:

HP original Part number: 319603-001

GEHC FRU Part Number: 5129534-3

NOTE

The FRU 5129534-3 is not managed by AW modality. Alternatively, this battery can be purchased from your local HP dealer, or any PC or Photo shop.

To replace the battery coin, refer to section "Battery" in the HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009 or section "System battery" in the HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009.

7.6.11.1 RTC battery removal

- Power down the server and remove the power cord from the electrical outlet.
- Remove the access panel (see [7.6.5 Opening the side cover on page 458](#))
- Remove any PCI card blocking access to the battery if applicable).
- Press the retaining clip with a flat-bladed tool to release the battery.
- Lift the battery out of the socket.

7.6.11.2 RTC battery replacement

- Press the new battery into the socket.
- Replace the PCI card (if applicable).
- Replace the access panel.
- Reconnect the power cord and turn on the server

7.6.12 Swapping the ML350 CPU box

NOTICE

The FRU ML350 G6 CPU box is delivered **without hard disks and with two power supplies**. Use the 6 x 500GB hards disks from your defective Unit. **If you are not confident** that **only** the CPU box is defective, make sure to order as well new Hards disks.

7.6.12.1 Field supplied tools

- One (foldable) hand cart to move the server safely, for one FE alone.

CAUTION



The weight of the complete ML350 CPU box is above the limit fixed by EHS specifications. Therefore, if handled by one FE alone, it must be moved and put into place by means of a transport hand cart. Refer to [A.11 HP ML350 server handling procedure on page 497](#) for safely handling the ML350 CPU box, according to EHS regulations.



7.6.12.2 Swap procedure

To replace the ML350 server CPU box by the FRU ML350 CPU box, proceed as follows:

1. Carefully remove the 6 HDDs from your defective ML350 CPU box, making sure you store them in the right order, so that you do not lose the RAID configuration and OS load. We recommend that you label the disks with a number when removing them.

NOTE

If you use the original HDDs from the old CPU box, with your new FRU CPU box, you will not need to reload the software. However, you will have to configure the iLO service processor and re-configure the hospital network and Time zone. See the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

NOTE

If you are NOT going to use the original 500GB HDDs from the old CPU box, you must also order new 500GB HDDs, and you will need to reload the software.

In both cases, you will have to calculate the new license keys corresponding to the license ID of the FRU CPU box. See [Step 11](#).

2. Open carefully the FRU ML350 CPU box packaging. You will need to re-use this packaging for sending back the defective unit.
3. Swap the defective ML350 CPU box with the FRU ML350 CPU box.
4. Carefully insert the 6 x 500GB HDDs, making sure to put them in the right order. Refer to the AW Server 3.2 Hardware Installation Manual if needed.

5. If you have chosen to keep the existing hard disks, reconfigure the ethernet ports, following next steps. In the other case, jump to [Step 11](#).
6. Open a Terminal, login as **root**.
7. Remove the `70-persistent-net.rules` file with the the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
8. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

9. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual at Job Card IST001B - Virtual Machine creation.
 - b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **Disable Hyperthreading**.
10. Re-configure the Hospital network and Time zone. Follow instructions given at Job Card IST005 - Network and Time Configuration.
11. Calculate new license keys. Use eLicense to calculate the new license keys, or contact your support center with the new CPU box license ID. See Licensing.
12. Default password for the iLO: Refer to the AW Server 3.2 Hardware Installation Manual to check or create the default password for the iLO service processor.
13. Load AW Server. As the FRU Low Tier server is not preloaded, refer to Sections Software upgrade to Final tests and system handover to customer to load the system with AW Server OS, platform, applications and to configure the AW Server.
14. Labelling: when the new ML350 CPU box is fully loaded, place the labels delivered within the FRU package on the new CPU box, referring to the included document, and/or refer to the AW Server 3.2 Hardware Installation Manual, Job Card IST007 - Installation of GEHC Product Labels.
DO NOT FORGET to place an EHS safety label as well.
15. e-IFU labelling: If delivered with the FRU unit, and for European sites only, stick the e-IFU label as well.
16. Ship back the defective CPU box: Use the FRU packaging to ship back the defective ML350 CPU box (refer to [A.11 HP ML350 server handling procedure on page 497](#)).

NOTICE

Use caution for **safely handling the ML350 CPU box, according to EHS regulations.**

17. Returning instructions:

The defective unit must be sent back (without hard disks and with its TWO power supplies) through the "SWAP (Supplier Warranty Program) process". Fill the red label identifying the defective unit with the following information:

- GEHC part number

- Job number
- Failure description. I.e : Result of Insight diagnostics tool summary if appropriate (see Chap 4, TSG005)
- Workstation Serial number (even for disk drives returned separately)
- FE contact name and ID number
- SWAP/FOI/FOA : Cross Swap Box

NOTICE

DO NOT retain any part from the old unit. Missing parts will be charged to your region.

7.7 High Tier Servers Hardware Disassembly/ Reassembly Procedures

Servicing the HPE ProLiant DL580 G7 Server / HPE ProLiant DL560 Gen8 Server / HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server High Tier Hardware is under the full responsibility of the vendor. This section is provided for reference.

Refer to [7.8 HP Escalation and Communication Flow on page 464](#) for contact details.

NOTICE

When calling the HP support center for replacement of a defective HPE R/T3000 UPS or KVM, prepare the Serial number of the HPE ProLiant DL580 G7 Server, HPE ProLiant DL560 Gen8 Server or HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server, as the serial number of these components are not tracked by HPE, and specify that **you request on-site assistance** for the replacement. Otherwise, the defective part may be sent to the site without HP Engineers on-site support.

NOTE

The Network Switch has a standard warranty.

7.7.1 Electrical Precautions

CAUTION

No LOTO procedure as such is applicable to the HPE ProLiant DL580 G7 Server / HPE ProLiant DL560 Gen8 Server / HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server as the internal voltages of the server correspond to those of a standard "plug and cord" workstation with no residual energy. Service procedures are thus deemed to carry negligible risk. However, FEs must begin any service intervention that requires opening the server case with the following procedure.

1. Perform the server shutdown procedure, preferably from the AW Server Service Tools, OR by depressing the On/Off switch on the front panel.
2. Disconnect the two power cords (HPE ProLiant DL560 Gen8 Server / HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server) or the four power cords (HPE ProLiant DL580 G7 Server) from the electrical outlet and then from the server.

3. Remove the two power cords (HPE ProLiant DL560 Gen8 Server / HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server) or the four power cords (HPE ProLiant DL580 G7 Server) and any spare power cords from the vicinity of the server, storing them in a safe place.

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of other important precautions to take.

7.7.2 De-racking High Tier Servers

CAUTION



The HPE ProLiant DL580 G7 Server CPU box weighs approximately 40kg (89 pounds)! The HPE ProLiant DL560 Gen8 Server CPU box weighs approximately 28kg (61 pounds) and the HPE ProLiant DL360 Gen9 Server / HPE ProLiant DL360 Gen10 Server CPU box weighs approximately 15kg (33 pounds). Comply with the HP safety recommendations provided in the section "Remove the server from the rack" or equivalent in the corresponding HP Service and Maintenance Guide, for instance the HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005.

7.7.3 Replacing High Tier Servers Components

Comply with the component-specific procedure provided in the chapter "Removal and replacement procedures" or equivalent in the corresponding HPE Service and Maintenance Guide:

- HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404
- HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008
- HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005
- HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005

7.7.4 Re-configuring the network after a network card replacement

In case of network card replacement by the Vendor, proceed to the following steps to re-configure the hospital network:

1. Open a Terminal, login as **root**.
2. Remove the **70-persistent-net.rules** file with the following command:
`/bin/rm -f /etc/udev/rules.d/70-persistent-net.rules <Enter>`
3. Reboot the server.
`reboot <Enter>`

NOTICE

Before performing a shutdown or reboot, refer to [4.2 Maintenance Mode on page 388](#) for details of important precautions to take.

4. Configure the iLO service processor:
 - a. Press **<F8>** when prompted during the boot sequence and follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST001B - Virtual Machine creation.

- b. Disable Hyperthreading settings in the BIOS.
 - c. Press **<F9>** during boot-up to enter BIOS menu. In **System Options > Processor Options**, select **Hyperthreading**, then select **DisableHyperthreading**.
5. Re-configure the Hospital network and Time zone. Follow instructions given in the AW Server 3.2 Installation and Service Manual, Job Card IST005 - Network and Time Configuration.

7.8 HP Escalation and Communication Flow

NOTICE

This section is **only applicable for the HP High Tier Server**.

7.8.1 HP Support Center Web site

When a hardware issue has been identified or is suspected on your HP High Tier server, you need to call the HP service in order to have the hardware part being replaced on-site.

See [7.8.2 HP supported countries telephone list on page 465](#) for the list of HP support phone numbers.

NOTICE

When calling the HP support center for replacement of a defective **UPS or KVM**, prepare the Serial number of the server, as the serial number of these components are not tracked by HP, and **specify that you request on-site assistance** for the replacement. In the other case, the defective part may be sent to the site without HP Engineers on-site support.

NOTE

The Network Switch has a standard warranty.

It is also possible to open service calls from the HP Web site, after being registered. Follow the procedure described below to register and/or request assistance.

- Connect to HP Web site
- Open the Navigator on HP Support Center: www.hp.com/go/hpsc
- Login or Register (if not done yet) on HP Web site
- Using the tab 'My HP Support Center', register for a new account or login
- Create a case on HP Web site
- Using the tab "Support option" and the sub-menu "Get help from HP", click on "Submit or manage support cases"
- Enter the serial number of the server or the serial number of the failed KVM or UPS component (may need to enter the serial number of the server) and click on 'Submit case'.
- Fill-in the issue information
- Write down the case number for future use.

NOTE

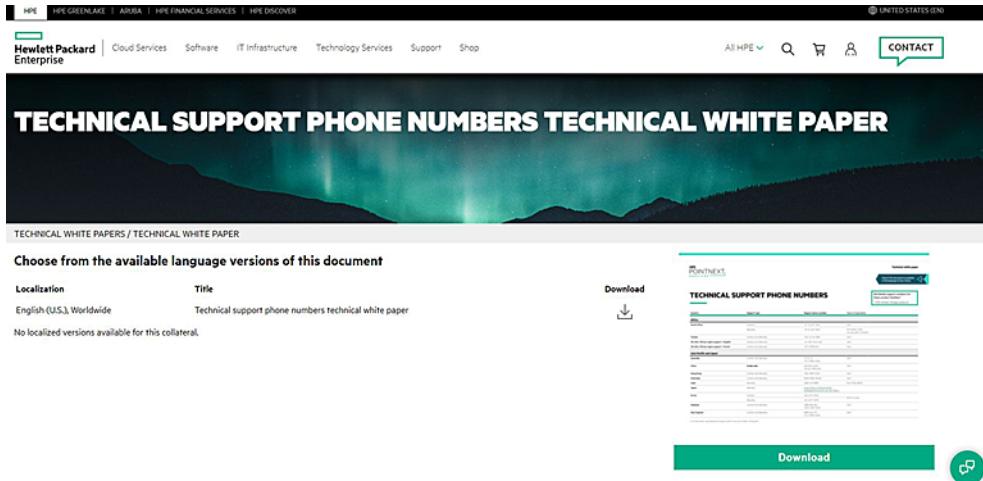
There will be no confirmation mail from HP web site.

- To follow the case
- Using the tab "Support option" and the sub-menu "Get help from HP", click on "Submit or manage support cases"

- Enter the case number and follow the status.

7.8.2 HP supported countries telephone list

- Go to <https://www.hpe.com/psnow/collection-resources/a00039121ENW>.
- Choose from the available language versions of the technical support phone numbers.



- Click **Download**.

7.9 Hardware Vendor Information Links

7.9.1 HP Hardware Vendor Information Links

Description	Link
Hewlett Packard Enterprise Home Page	https://www.hpe.com/
Hewlett Packard Enterprise Support Center	https://support.hpe.com/hpsc/public/home
HPE ProLiant DL360 Gen10 Server - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=a00018808en_us
HPE ProLiant DL360 Gen9 Server - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c05031449
HPE ProLiant DL560 Gen8 Server - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c05062110
HPE ProLiant DL580 G7 Server - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c05282198
HPE ProLiant ML350p Gen8 Server - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c03908833
Intelligent Provisioning User Guide for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=a00017037en_us
Intelligent Provisioning User Guide for HPE ProLiant Gen9 Servers and HPE Synergy	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=c04419967
HPE Integrated Lights Out (iLO 5) for HPE Gen10 Servers - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=emr_na-a00019271en_us
HP Integrated Lights-Out 4 (iLO 4) - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=emr_na-a00043732en_us
HP Integrated Lights-Out 3 (iLO 3) - Document List	https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=emr_na-a00044678en_us

7.9.2 Note about the HP Serial number

NOTE

The serial number is 10 characters *CCSYWWXXXX* encoded using:

- *CC*: Country Code (ex: GB -> Great Britain, CZ -> Czech Republic...)
- *S*: Site Code Designator (ex: 8)
- *Y*: Year (ex: 9 -> 2009, 0 -> 2010, 1 -> 2011...)
- *WW*: Week or the year in ISO format (ex: 01, 02, 30, 52)
- *XXXX*: Code to create a Unique Identifier

Chapter 8 Other documentation and web links

8.1 VMware documentation

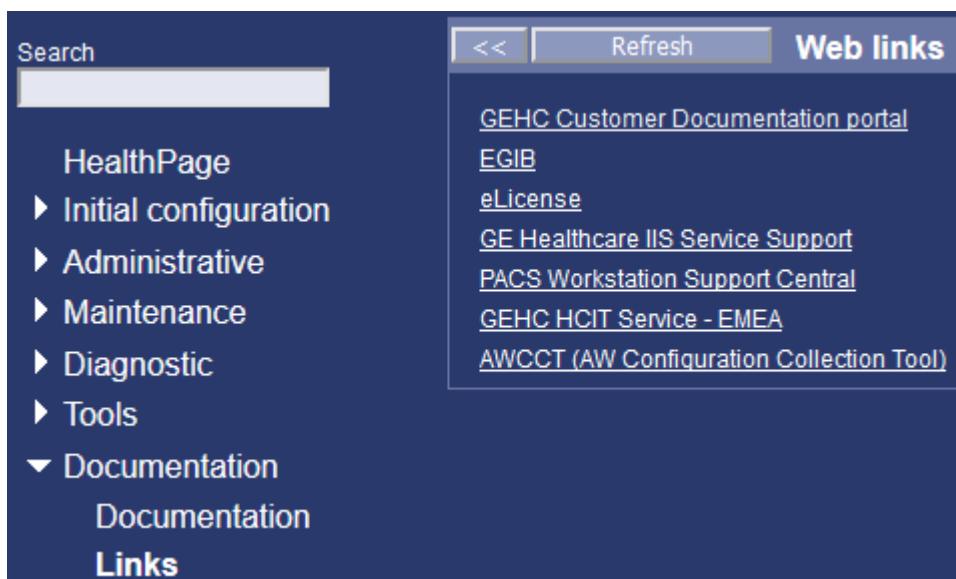
For VMware documentation, see: <https://www.vmware.com/support/pubs/>

Other country-specific versions of the site are available.

8.2 Web links

- In the AW Server Service Tools, click on **Documentation > Links**.

A list of Web links useful to Service displays.



The available links are:

- **GEHC Customer Documentation portal**
- **EGIB**: link to the Global EGIB (<http://gib.gehealthcare.com>)
- **eLicense**: link to the software license generation tool
- **GE Healthcare IIS Service Support**
- **PACS Workstation Support Central**
- **GEHC HCIT Service - EMEA**
- **AWCCT (AW Configuration Collection Tool)**

8.3 Universal Viewer and Centricity PACS documentation

NOTE

The following documents are available in the Customer Documentation Portal:
Service Documents for the Universal Viewer:

- Universal Viewer Installation Manual

- Universal Viewer Site Configuration Tool Service Manual
- Universal Viewer Administrator Manual

Service Documents for Centricity PACS:

- Centricity PACS Servers Service Manual
- Centricity PACS Servers Installation and Upgrade Manual
- Centricity PACS Workstation - Installation and Service Manual
- Centricity PACS System Administrator
- Centricity PACS System Overview Manual

Appendix A Appendices

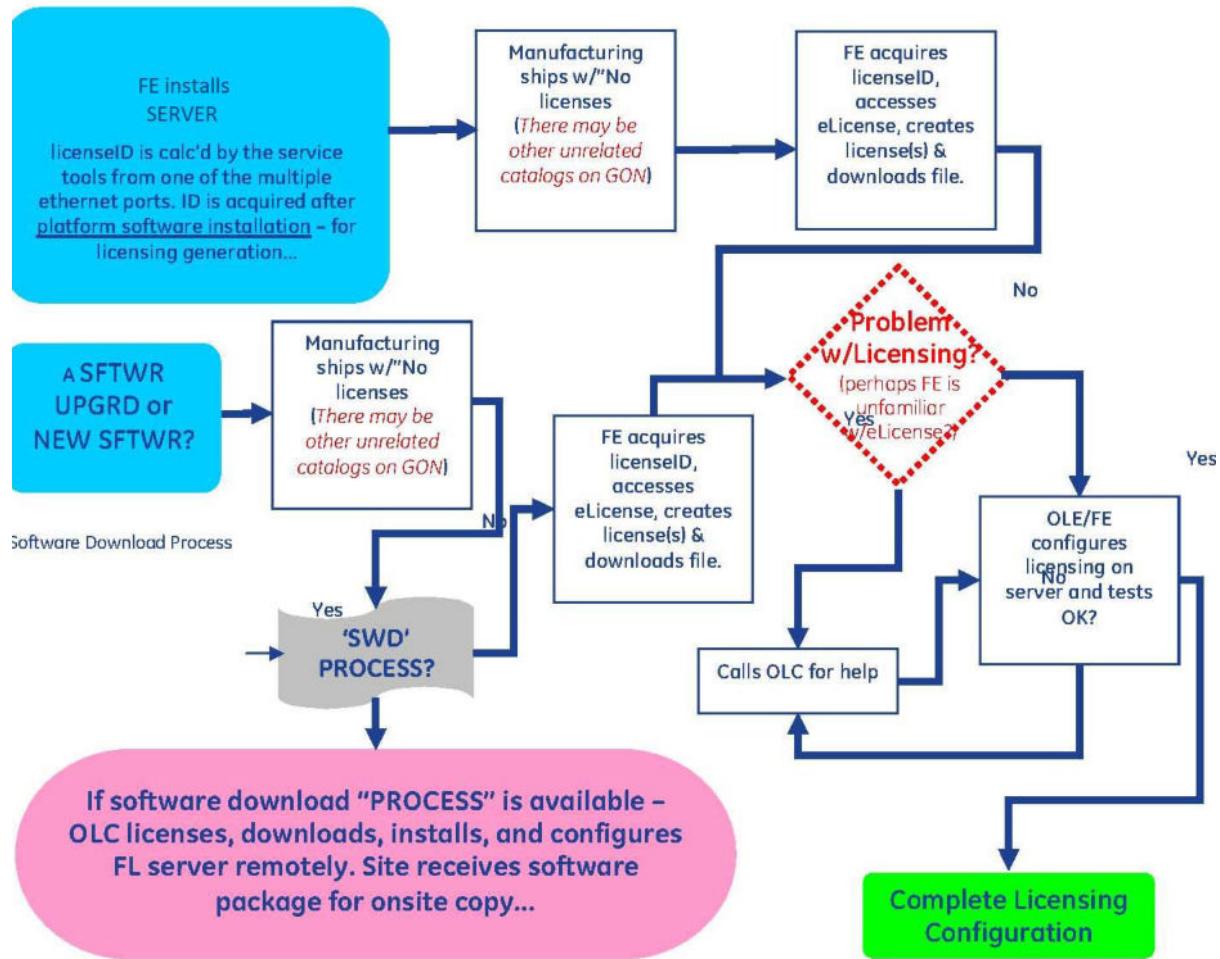
A.1 Overview

This chapter covers the following items:

- [A.2 AW Server Licensing on page 469](#)
- [A.3 Hardware Vendor Information Links on page 470](#)
- [A.4 WGET on page 470](#)
- [A.5 Users, Groups, Roles and Members on page 473](#)
- [A.6 Password Change on page 484](#)
- [A.7 Setting Date and Time on page 486](#)
- [A.8 Command Line Tools on page 491](#)
- [A.9 Definitions and Acronyms on page 493](#)
- [A.10 Command-Line Interface on page 495](#)
- [A.11 HP ML350 server handling procedure on page 497](#)
- [A.12 Old systems return process after upgrade on page 500](#)
- [A.13 Filesystem Check on page 500](#)
- [A.14 Launching AWS CLIENT on remote OLE laptop on page 505](#)
- [A.15 BIOS / FIRMWARE upgrade on page 506](#)
- [A.16 HP DL580/DL560/DL360 Handling Procedure on page 511](#)
- [A.17 Secure Media Destruction Procedure on page 511](#)
- [A.18 Application Profiles for AW Server on page 511](#)
- [A.19 Re-configuring Corrupted Serial Number on page 511](#)
- [A.20 Sun High Tier X4450 returning Procedure on page 512](#)
- [A.21 Installing/renewing an AW Server external CA signed certificate on page 514](#)
- [A.22 Hardware Security on page 517](#)
- [A.23 RPM2CPIO on page 528](#)
- [A.24 AW Server enhanced security configuration on page 529](#)

A.2 AW Server Licensing

System licenses are not created by Manufacturing, and will thus need to be created by the GEHC FE or the OLC for the FE at server platform installation time.

**NOTE**

GERU/SWD: This scenario is not available for GEHC-IT environment.

For further details and examples of licensing, see the AW Server 3.2 Installation and Service Manual, Job Card IST008 - Initial Configuration and Licensing.

A.3 Hardware Vendor Information Links

Refer to 7.9 Hardware Vendor Information Links on page 465.

A.4 WGET

Another tool that is very useful for basic NETWORK connectivity testing and beyond is **wget** (**World Wide Web Get.**)

Wget is a computer program that implements simple and powerful content retrieval from web servers. It currently supports downloading via HTTP, HTTPS, and FTP protocols, the most popular TCP/IP-based protocols used for web browsing. Its features include recursive download, conversion of links for offline viewing of local HTML, support for proxies, and much more.

- "wget" is not a GEHC service tool.
- "wget" is a downloadable software package that can be acquired as "freeware" on the Internet, downloaded and installed on your Windows® PC, and / or the AW Server client PC in question.
- "wget" is already part of the server Linux OS tool-set.

One of the ways that **wget** can be used to as part of AW Server network testing or trouble-shooting, is to (**from the client**) attempt to download the **AW Server Windows® client software**. Doing this

from a client PC is essentially the same thing that is done when the client first accesses the server to get the client application, see installation validation tests in AW Server 3.2 Installation and Service Manual, Job Card IST014A - Standard Client PC installation & Tests.

This means that you will need to either have access to the CLIENT PC – or – work with the site admin or user to run this test.

If the issue at hand is that the client cannot download and run the client software package, this type of testing is especially useful because it uses the same HTML / FTP communication channels that the application is trying to use.

USE CASE EXAMPLE 1 - Successful example from the Windows® Client PC

- Command-line

```
C:\Program Files\GnuWin32\bin> wget http://3.57.48.64/client/AWE-windows-setup.exe --15:19:07-- http://3.57.48.64/client/AWE-windows-setup.exe
```

- Tool feedback & results=> `AWE-windows-setup.exe'

Connecting to 3.57.48.64:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 89,842,702 (86M) [application/octet-stream]

100%[=====] 89,842,702 4.63M/s ETA
00:00

15:19:27 (**4.32 MB/s**) - `AWE-windows-setup.exe' saved [89842702/89842702]

- Conclusion(s)

NOTE

The segmented results – connected > HTTP request > progress indicator > completion with bandwidth data – 4.32 MB/s.

- Basic connectivity = **GOOD**
- HTTP stack request and progress = **GOOD**
- Performance – network speed = **Moderate.**
- Minimum network spec = 100Mbps
- Minimum recommended Intranet/LAN bandwidth = 40Mbps
- The AWS Client Checker "Network Test" uses the following criteria for its client bandwidth analysis:
- **<3Mbps = FAIL**
- **3 to 6Mbps = MODERATE**
- **>=6Mbps = GOOD**

USE CASE EXAMPLE 2 - Unsuccessful example from the Windows® Client PC

- Command-lineC:\Program Files\GnuWin32\bin> wget http://3.57.48.64/client/AWE-windows-setup.exe --15:19:07-- http://3.57.48.64/client/AWE-windows-setup.exe

- Tool feedback & resultsConnecting to 3.57.48.64:80... failed: Connection timed out.Retrying.

- Conclusion(s)

NOTE

Connection timeout means that basic network connectivity is NOT established. In this case, the "ping" tool should have also failed.

- If other clients are connecting OK – chances are the NETWORK is OK, and this issue has to do with the basic network setup on the particular **CLIENT**.
- If other clients on the network also cannot connect – the **NETWORK** is probably at fault.

USE CASE EXAMPLE 3 - Successful example from a Linux box

Another way to test - if the actual client PC cannot be used - is to identify and use a "Linux" box – like an AW – on the same or similar site subnet as the PC client.

- **Command-line** – from the AW

```
{csexw8000}[18]# wget http://3.70.208.33/client/AWE-windows-setup.exe
--07:18:05-- http://3.70.208.33/client/AWE-windows-setup.exe
```

- **Tool feedback & results**

```
=> `AWE-windows-setup.exe'
```

Connecting to 3.70.208.33:80... **connected. HTTP request sent, awaiting response... 200 OK**

Length: 89,846,621 [application/octet-stream]

100%[=====] 89,846,621
10.35M/s

ETA 00:00

07:18:14 (**9.90 MB/s**) - `AWE-windows-setup.exe' saved [89,846,621/89,846,621]

- Conclusion(s)

- **Basic connectivity, ftp, and bandwidth if GOOD.**

- In this case – most likely with the **NETWORK** is OK.
- The particular **CLIENT** in question probably has a network or other configuration issue.

USE CASE EXAMPLE 4 - Unsuccessful example from a Linux box

Another way to test - if the actual client PC cannot be used - is to identify and use a "Linux" box – like an AW **or another server** – on the same or similar site subnet as the PC client.

- **Command-line**

```
ct-demo-aws:/export/backup # wget http://3.70.211.88/client/AWE-windows-setup.exe
--15:27:47-- http://3.70.211.88/client/AWE-windows-setup.exe
```

- **Tool feedback & results**

```
=> `AWE-windows-setup.exe'
```

Connecting to 3.70.211.88:80... connected. HTTP request sent, awaiting response...

404 /awe/client/AWE-windows-setup.exe 15:27:47 **ERROR 404:** /awe/client/AWE-windows-setup.exe.

- Conclusion(s) Able to connect, but **404 error**.

- The **404 or Not Found** error message indicates that the client (a Linux box in this case) was able to communicate with the server but either the server could not find what was requested, or it was configured not to fulfill the request and did not reveal the reason why. **404 errors should not be confused with "server not found" or similar errors, in which a connection to the destination server could not be made at all.**
- In this case, if it is not known for sure that the target AW Server stand-alone test is OK, there might be an issue on the target AW **SERVER** in that the requested application file (AWE-windows-setup.exe) is not available, is a different name, or is in a different file location. Make sure the file is there, and that you have the correct path.

- In this case, if it is known that the target AW Server stand-alone test is OK, this result might mean that the **NETWORK** has some configuration that is blocking the file discovery & file transfer portion of the connection.
- The point is – in this case – you have a PC CLIENT that does not work, and you **have now tested an available "Linux box" client on the same or similar subnet that also does not work**. If the target AW Server stand-alone test is OK – you still cannot **completely** eliminate the target server, because this 404 error simply means the requested file was not found for some reason. But, the chances are that the **NETWORK** is at issue.
- The best way to finally eliminate the target server is to find another client that CAN successfully find and download the file...

Disclaimer:

"wget" is not the only tool that can be used for this purpose. There are other tools and other methods for network analysis and testing. There is no one-size-fits-all tool or method, and no one GEHC endorsed equivalent. Use this information to the extent that it can help your particular need.

Also, it is not intended or implied that this small guide will help resolve ALL NETWORK issues.

The goal of ALL AW Server trouble-shooting scenarios is to:

- Validate the server by itself with the stand-alone testing process.
- Use multiple clients on multiple sub-nets to verify and/or isolate the nature or extent of the issue.
- if the issue cannot be reasonably linked to the server after all of this - engage the customer's network admin to help resolve the problem, and make any appropriate suggestions about the root cause of the issue if you can.

A.5 Users, Groups, Roles and Members

A.5.1 Groups, Roles and Members Example Matrix

User/Member NOTE It is recommended to NOT create User ID's with "spaces" in the name	Group	Access Level	Definition
MaryMarche	Field Engineer (FE) - geservice	GE Service	Access to all tools.
EllaEnrich Samantha Smith LamarLopez	Technologist/IT - admin	Administrator	Greatest access to all features and tools with the exception of Service Tools.
RalphRogers JoeJohnson	Radiologist -standard	Standard User	General access for most users. Can see database and access user tools, but not administrator or Service Tools.

AndreaAnderson KateKruthers BillBurton DavidDavidson	Referring Physician -limited	Limited User	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.
---	------------------------------	---------------------	--

A.5.2 Example User/Role Matrix

- **1 member** – (Mary) belongs to the FE group, and has service level privileges and can access service, administrator and standard user tools.
- **3 members** – (Ella, Samantha and Lamar) belong to the Technologist/IT group, and have administrator privileges and can access administrator and standard tools.
- **2 members** – (Ralph and Joe) belong to the Radiologist group, and have standard privileges and can access only standard user tools.
- **4 members** – (Andrea, Kate, Bill and David) belong to the Referring Physicians group, have limited privileges and cannot access any user tools.
- You can create any number of local users and groups with any name(s) meaningful to you.

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

If the site has an **active-directory/LDAP server** (for example, user ID, billing, email, intra-, internet access, etc.), and the site wishes to use its account configuration, you must configure the server connection via the **Enterprise Tab**. In addition, you must make sure the group from the active directory/LDAP server is mapped – or created as an enterprise group in EA3.

There are essentially TWO ways to establish USER ACCOUNTS:

1. **Local** USER ACCOUNTS
2. **Active Directory/LDAP** or Enterprise USER ACCOUNTS

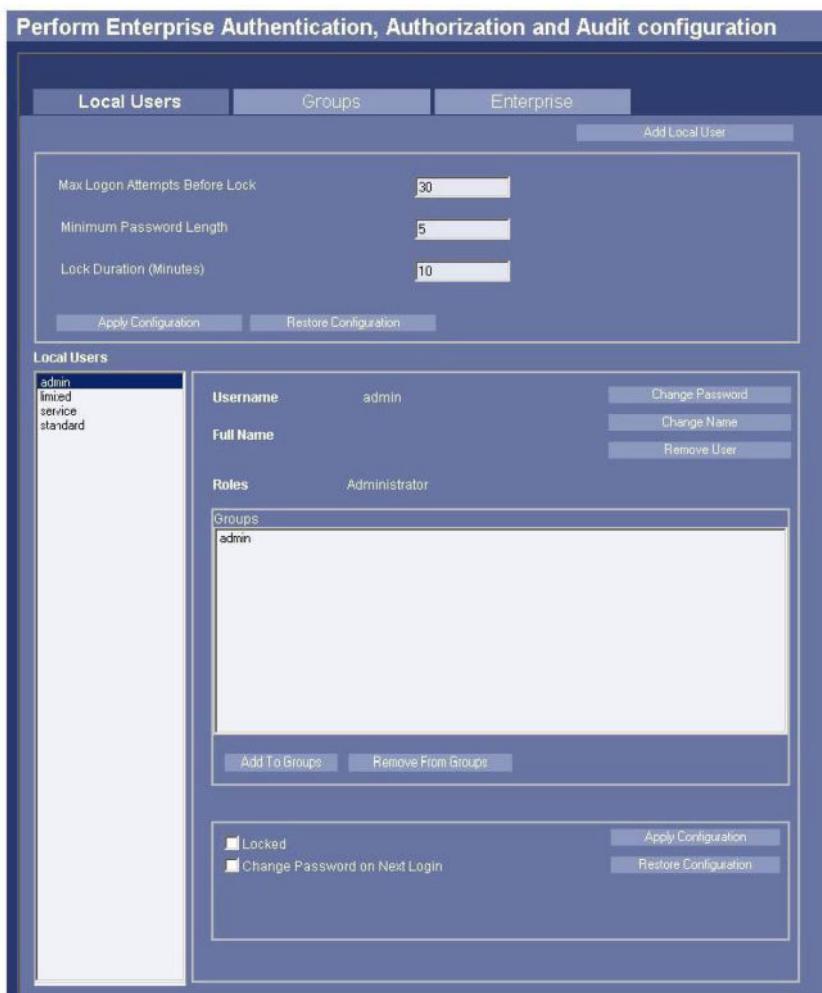
It is recommended to use one approach or the other for individual users, to avoid potential group permission conflicts, and unnecessary administrative complexity.

A.5.3 Local Users Tab

NOTE

In case of Full integration or Seamless integration, all user authentications are done by PACS, and all users authenticated by PACS have Standard rights. These passwords should be changed even in Seamless integration.

This is the entry page to the Users (EA3) tool.

Figure A-1 USERS (EA3) – LOCAL USERS TAB

There are FOUR **BUILT-IN "local"** accounts, each with an assigned ROLE that corresponds to the account name:

- admin account = Administrator Role (Almost ALL Service Tools access)
- limited account = Limited User Role (No service tool access)
- service account = GE Service Role (ALL Service Tools access)
- standard account = Standard User Role (Few Service Tools access)

The default login names and passwords for the built-in local Service Tool accounts shall be changed to unique, complex passwords at installation time (refer to [1.3.1 Password Management on page 40](#)).

NOTICE

TO PROTECT CUSTOMER SECURITY, ALL DEFAULT PASSWORDS 'MIGHT' NEED TO BE CHANGED DURING INSTALLATION IF SITE IT REQUESTS. THIS APPLIES TO BOTH THE LINUX OS PASSWORDS AND THE AW SERVER USERS PASSWORDS. SEE [A.6 Password Change on page 484](#).

A.5.4 Factors to Consider when Creating Local Users Accounts

- If the site does NOT have an enterprise account policy or authentication server infrastructure, by default they will be using all **LOCAL** accounts, and this tool will be the main account management interface.
- **IT IS RECOMMENDED TO NOT CREATE USER ID NAMES WITH "SPACES" IN THEM.**
- If the site has an enterprise account policy or authentication server infrastructure, and wants to use it – use the Local Users tool to only manage the creation of local site IT or service access accounts – not site users, as these you will configure via the enterprise users tab.
- It is advisable to setup at least one local account for the site IT or Account Admin who will be responsible for managing site accounts. If the individual can be with you as you do this, this will serve as a good training session for them, as well as set them up for admin responsibilities.
- The logins and passwords for the default built-in accounts should be reserved for GE knowledge and use only. However, if the site IT Admin objects to the default accounts / passwords, the passwords can be changed per the site's policy. (see [A.6 Password Change on page 484](#)).
- Additionally, if the customer objects to all of these built-in accounts, you can consider deleting the standard, limited, and admin accounts. The service account cannot be deleted, and is permanently required for GEHC service use.

NOTICE

IF PASSWORDS ARE CHANGED YOU MUST NOTIFY THE GEHC ONLINE SUPPORT CENTER SO THAT THE NEW PASSWORD(S) ARE RECORDED CORRECTLY FOR REMOTE SERVICE NEEDS. THERE MUST NEVER BE A SITUATION WHERE REMOTE SERVICE IS LOCKED-OUT FROM EMERGENCY SERVICE DUE TO AN UNKNOWN PASSWORD CHANGE! (see [A.6 Password Change on page 484](#)).

Other account variables are available for setup at this time as you can see in the Local Users tool window. Configure these as necessary – or not. When done, click on **Apply Configuration**. A **GREEN** indication should display momentarily directly beneath the Apply and Restore buttons if the apply action is successful.

- If it is not successful, this could mean that there is something wrong with the data that was entered in the tool, or with the system in general.
- Perhaps attempt another simple and default account creation, and see what happens.
- Or remove the new account, re-create it, and try the apply again...
- The **Restore Configuration** will restore the last applied configuration.
- Example – if you have configured a new user, but have not successfully applied it yet, the Restore button will reload the current or last configuration – losing the new one. The new one will not be available for Restore until it is successfully Applied.

A.5.5 Groups Tab

In order for a new user (local or enterprise) to have proper access to the server applications and/or tools, the user must be assigned a **ROLE** – which by definition determines their access privileges. The way to do this is to add the new user – or the new enterprise user's GROUP to the existing **BUILT-IN ROLES** – Administrator, Limited User, GE Service, or Standard User.

NOTICE

No ROLE assignment defaults to CLIENT 'STANDARD' USER ROLE

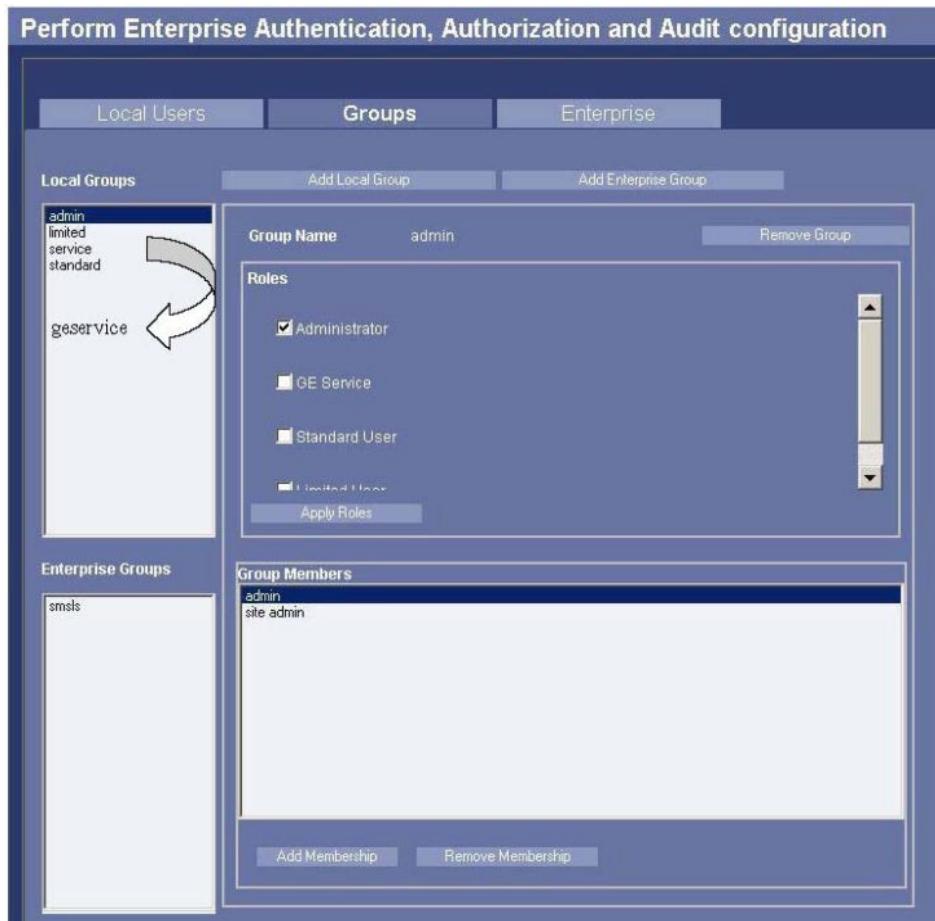
NOTICE

No ROLE assignment defaults to SERVICE TOOLS 'LIMITED' ROLE

NOTICE

No ROLE assignment = standard

Figure A-2 USERS (EA3) – GROUPS TAB



Other account variables are available for setup at this time as you can see in the Groups tool window. When done, click on **Apply Configuration**. A **GREEN** indication should display momentarily directly beneath the Apply and Restore buttons if the apply action is successful.

- If it is not successful, this could mean that there is something wrong with the data that was entered in the tool, or with the system in general.
- Perhaps attempt another simple and default account or group configuration, and see what happens.
- Or remove the new data and try the apply again...
- The **Restore Configuration** will restore the last applied configuration.
- Example – if you have configured a new user or group, but have not successfully applied it yet, the Restore button will reload the current or last configuration – losing the new one. The new one will not be available for Restore until it is successfully applied.

- This Restore Configuration button does NOT restore "system" configuration...

A.5.6 "Role" Process Flow for Local Users

NOTE

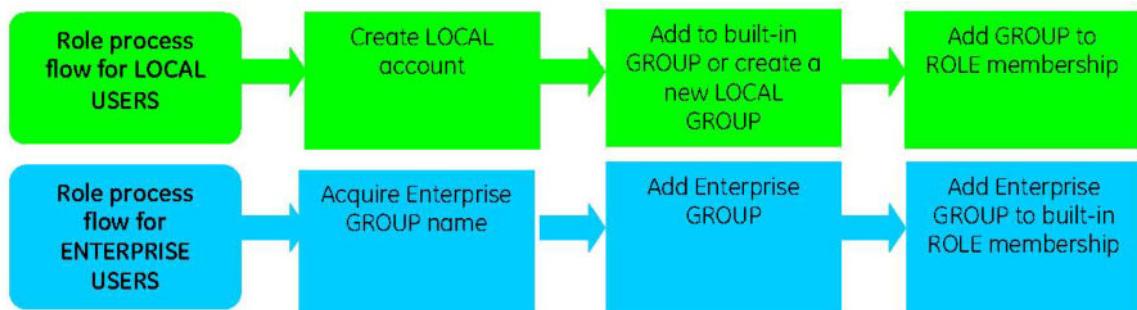
In case of Full integration or Seamless integration, all user authentications are done by PACS, and all users authenticated by PACS have Standard rights, so there is no specific Process Flow to follow on AWServer in that case.

- **Local Users** must be added to one of the built-in groups in the **Local Users tab** – via the **Add To Groups** button.
- Or, a **NEW GROUP** needs to be created with the **Add Local Group** button in the Groups tab, and the **Local User** must be added to it.
- The **BUILT-IN GROUP** will already have an assigned built-in ROLE, so nothing more is needed.
- But, for the new **Local GROUP**, it must now be assigned membership in one of the **BUILT-IN ROLES** using the **Add Membership** button in the **GROUPS tab**.

A.5.7 "Role" Process Flow for Enterprise Users

- **Enterprise Users** must already be members of an enterprise group setup by the site enterprise account admin. So, they do not need to be added to any of the server's built-in groups.
- The Enterprise GROUP must now be added to the membership of one of the server's BUILT-IN ROLES via the **Add Enterprise Group** button in the Groups tab.
- Depending on the Role that the enterprise group is added to, will determine the access privileges for any user who is a member of the group.
- **Most users will and SHOULD BE assigned to the Standard User Role.**
- **Be very careful here! The server's tools are designed to give appropriate access to Service Tools based on these built-in roles!**

Figure A-3 USERS (EA3) – ROLE PROCESS FLOW



A.5.8 Enterprise Tab

Click on the **Enterprise** Tab. The following screen should display.

NOTE

If the site uses an Enterprise Server, related information is normally supplied by the IT Admin or site User Admin during the initial site survey and recorded in the Preinstallation checklist. If there is no Enterprise server data in the survey document – the only account configuration that can be done are Local User Accounts Configuration.

Figure A-4 USERS (EA3) – ENTERPRISE TAB

The **Enterprise** Tab allows to configure the Enterprise user(s) accounts.

- General Enterprise Server setting:

At the top of the page select the appropriate settings:

- Enable Enterprise Authentication:** Enable this to allow enterprise users to access the server.
- Cache Enterprise Users:** Enable this to allow successful enterprise logins to continue to work even if the Enterprise Server is unavailable (the site's IT admin should make this decision). This will maintain until the AW Server is rebooted.
- Enterprise Authentication Latency (Seconds):** Set this time consistent with the normal expected time that the Enterprise Server can process a successful login. If too short, it will timeout the login request before the login can be completed. If too long, it will keep trying even though it cannot login.

- Enterprise Server configuration:

There are two ways to configure the Enterprise Server:

- Semi-Automatic Configuration:** Follow the steps in the **Configuration Instructions** panel on the left side of the page. This will automatically enter configuration data into the right-hand panel. If this method does not complete successfully, use manual configuration.

- **Manual Configuration:** Use the information from the site survey document and/or the IT admin to manually fill in the correct entries in the right **Server Configuration** area and use the **Generate Defaults** button, in the **Configuration Instructions** panel, to complete the information in the **LDAP Configuration** area.

a. Server configuration:

Depending on the choices done in the **Authentication Type** field and in the **Use SSL** and **Verify Certificate** checkboxes, there are six types of Enterprise Active Directory/EA3 User Authentication configurations:

1- Simple LDAP, Use SSL and Verify Certificate unchecked

2- Simple LDAP, Use SSL checked, Verify Certificate unchecked

3- Simple LDAP, Use SSL and Verify Certificate checked

4- Kerberos, Use SSL and Verify Certificate unchecked

5- Kerberos, Use SSL checked, Verify Certificate unchecked

6- Kerberos, Use SSL and Verify Certificate checked

Server Configuration	
Server Name / IP	Hospital-DC01.training.hospital.edu
Authentication Type	Kerberos Kerberos Simple LDAP
	<input checked="" type="checkbox"/> Use SSL <input checked="" type="checkbox"/> Verify Certificate

For each of these authentication configurations here are the considerations:

1- Simple LDAP, Use SSL and Verify Certificate unchecked

Important

This uses no security and authentications will be in cleartext. This should not be used.

2- Simple LDAP, Use SSL checked, Verify Certificate unchecked

4- Kerberos, Use SSL and Verify Certificate unchecked

5- Kerberos, Use SSL checked, Verify Certificate unchecked

Secure exchanges of authentication will occur and no special certificate configuration is required on the AW Server. Simply configure and test the proper 'Server Configuration' details obtained from the site IT administrator contact.

3- Simple LDAP, Use SSL and Verify Certificate checked

6- Kerberos, Use SSL and Verify Certificate checked

This requires to import the certificate from the site's Active Directory server and its Certificate Signing Authority.

Follow the steps in section [A.5.8.1 Importing the site's Active Directory server certificate and its Certificate Signing Authority on page 482](#) to import the certificate.

- b. Click on **Apply Configuration**.
3. Verify that the Enterprise Server configuration was successful:
 - a. Click on **Test Connection** on left side of the page. If the connection is successful, the message **CONNECTION OK** (on a green background) appears briefly next to the button.

- b. Enter an enterprise **Username** and **Password**, then click the **Login** button on left side of the page. The **Login Results** area displays the result of the login and group.

Figure A-5 ENTERPRISE LOGIN -TEST RESULTS

The screenshot shows a step-by-step guide for enterprise login:

- Step 1:** Enter the Server Name / IP and the authentication type (at right). Click 'Test Connection'.
- Step 2:** Choose the Server Type from the drop-down (at right). Click 'Generate Defaults'.
- Step 3:** Make any necessary modifications to the default configuration.
- Step 4:** Attempt to login with your username/password to the Server. The fields show 'Username: aa039947' and 'Password: [redacted]'. A 'Login' button is present.
- Step 5:** Confirm there were no errors, and your correct name and group membership was returned. The 'Login Results' section shows:
 - Successful login for aa039947
 - Full Name: [redacted]
 - Group Membership: FS_cse_programs_1001339_C_Mbrs,FS_Apps_1006539_C_Mbrs
- Step 6:** If the configuration is ok, click 'Apply Configuration'.

NOTE

Along with the success or failure indication, other data of interest in this example is the information starting with – **Group Membership**. The data is setup by the administrator of the enterprise server, and is comma delineated. In this case example the group membership data needed is the last data set (scrolled-down) – **"smsls" This data will need to be entered in the Groups Tab as an Enterprise Group – and then assigned a Role**. Different configurations may have different formats, and strings. This is only an example.

NOTE

Also – there are various browser implementations that "might" cause the **scroll-bar** in the - Login Results - window to **NOT** show up or **NOT** be functional when there is data that goes beyond the normal window size. **The work-around is to use your left mouse button to select the text and drag down to the hidden information – which will act like scrolling, and display the information below the window boundary...**

- c. Make sure the enterprise accounts can successfully login to the AW Server Client Application.
- d. If the certificate from the site's Active Directory server has been imported, select the **Verify Certificate** checkbox and verify the successful login as in **Step 3.b** above.

The 'Server Configuration' dialog box contains the following fields:

- Server Name / IP:** DCLONUKP0102.logon.ds.ge.com
- Authentication Type:** Simple LDAP
- Checkboxes:**
 - Use SSL
 - Verify Certificate

4. Troubleshooting:

- If the tests in this tool work, but the Client Application will not login, it could mean that there is a failure in the client application on the client PC.
- If the test connection or test login in this tool fail, it could mean a server or network server configuration issue.
- If there is a time difference of more than 5 minutes between the Enterprise Authentication Server and the AW Server, the CLIENT login will fail – with an Enterprise Account Configuration (EA3) error message. In this case if you test the login with the Test Login Tool, the Login Results (see figure) will show a "CLOCK SKEW" error. Adjust the time on the AW Server to match the Enterprise Server – OR – configure NTP on the AW Server... see the Service section of this document for details...

A.5.8.1 Importing the site's Active Directory server certificate and its Certificate Signing Authority

This section describes how to import the certificate from the site's Active Directory server and its Certificate Signing Authority.

NOTE

From AW Server 3.2 Ext. 4.8, this procedure can be done using the Certificate Management page (Refer to the *AW Server 3.2 Installation Manual, Job Card IST010 - Administrative Configuration*).

1. Open the AW Server Console/terminal, login as **root**.

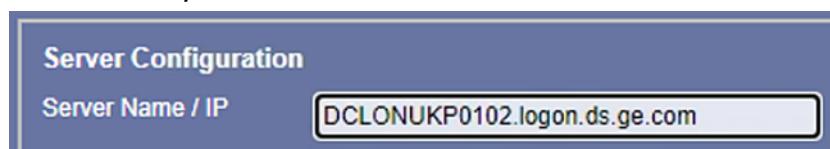
2. Navigate to the ea3 configuration directory:

```
cd /usr/share/gehc_security/ea3/configs <Enter>
```

3. Verify that you can access and obtain the certificate information from the hospital system using the following **openssl** command:

```
openssl s_client -showcerts -connect <Authentication_Server_FQDN>:636
<Enter>
```

Where **<Authentication_Server_FQDN>** is the full name of the hospital's authentication server Active Directory system. This should be obtained from the IT admin in charge of Enterprise Authentication. It should be the same as found in the site's AW Server from the Service Tools in **Administrative > Configuration > Users (EA3) > Enterprise** tab, in the **Server Name / IP** field.



For instance:

```
openssl s_client -showcerts -connect DCLONUKP0102.logon.ds.ge.com:636
<Enter>
```

NOTE

If this fails, verify the authentication server FQDN with site admin and verify the AW Server has the correct site DNS servers configured to resolve the FQDN from the Service Tools in **Maintenance > Network > DNS settings** tab.

4. Use the following `openssl` command to redirect the authentication server's certificates to a file called `authservercerts.pem`:

```
openssl s_client -showcerts -connect <authentication_server_FQDN>:636
</dev/null | sed -n -e '/-.BEGIN/,/.END/p' > authservercerts.pem
<Enter>
```

Where `<Authentication_Server_FQDN>` is the full name of the hospital's Active Directory authentication system as previously identified.

For instance:

```
openssl s_client -showcerts -connect DCLONUKP0102.logon.ds.ge.com:636
</dev/null | sed -n -e '/-.BEGIN/,/.END/p' > authservercerts.pem
<Enter>
```

5. Use the following command to separate multiple certificates into unique files:

```
csplit -szf authservcert- authservercerts.pem '/-----BEGIN
CERTIFICATE-----/' '{*}' <Enter>
```

NOTE

One or more files will be created, one for every certificate received from the authentication server. The files will be named sequentially as in the following example:

```
authservcert-00
authservcert-01
authservcert-02
```

6. List and verify how many unique certificates files were created using the command:

```
ls -al authservcert-* <Enter>
```

7. Import the first of the unique certificate files to a Java Key Store (jks) in the current AW Server ea3 configuration directory using the command:

```
echo yes | keytool -import -alias authservercert_00 -file
authservcert-00 -keystore clientTruststore.jks -storepass Pass1word
<Enter>
```

8. Repeat the previous command as many times as necessary to import any other certificate files to the Java Key Store. You may not need to repeat if there was only one file (`authservcert-00`) created.

For instance:

```
echo yes | keytool -import -alias authservercert_01 -file
authservcert-01 -keystore clientTruststore.jks -storepass Pass1word
<Enter>
```

```
echo yes | keytool -import -alias authservercert_02 -file
authservcert-02 -keystore clientTruststore.jks -storepass Pass1word
<Enter>
```

9. Copy the Java Key Store configuration to the `tls_config.properties` file using the command:

```
echo "tls.truststore=/usr/share/gehc_security/ea3/configs/
clientTruststore.jks" > tls_config.properties <Enter>
```

10. Change the file permissions on the `tls_config.properties` file using the command:

```
chown gehc_security:gehc_security clientTruststore.jks
tls_config.properties <Enter>
```

11. Restart the AW Server's tomcat and ea3 services using the command:

```
systemctl restart tomcat ea3 <Enter>
```

NOTE

If the command returns the following error:

```
-bash: systemctl: command not found
```

Please run the commands:

```
service ea3 --full-restart <Enter>
```

```
service tomcat6 --full-restart <Enter>
```

A.6 Password Change

The default passwords that come with the native hardware and software shall be changed during the installation procedure to increase security.

This applies to both the Linux OS passwords and the AW Server passwords.

The AW Server users passwords shall be changed as well, in case they have expired (default passwords lifetime is 60 days (in RMF mode) or 90 days in other modes).

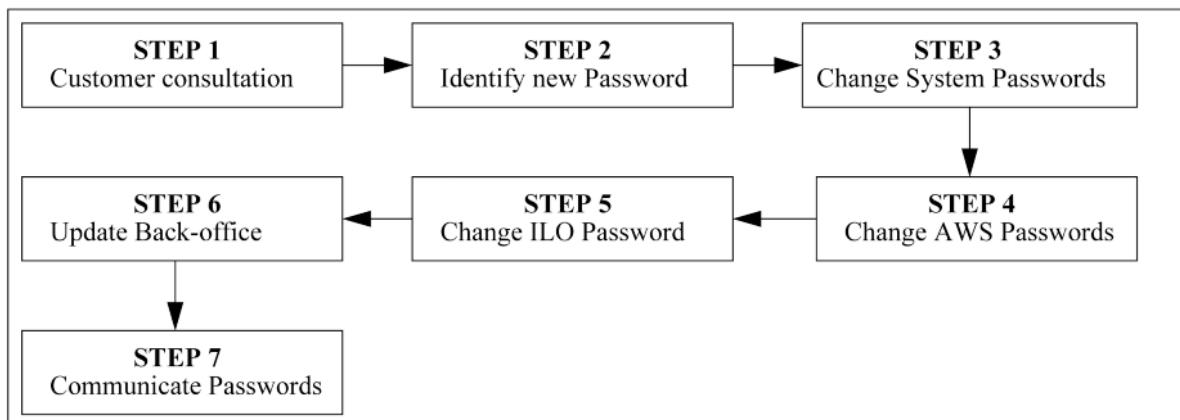
Some customer environments also require passwords to be changed at regular intervals. When passwords are changed, it is essential that the correct process and policy be followed – both from the customer's standpoint, and from a GEHC service support standpoint.

To make the AW Server system as secure as possible, GEHC recommends that the server's root password be changed at this point in the installation process. Changing to a password other than the default password will help minimize the chance of unauthorized users accessing the system.

When any passwords are created or changed, it is very important to involve both GEHC and the customer's IT admin person, and that the new passwords are recorded correctly for Remote service needs.

A.6.1 Process Overview

For **reference**: “System Password Change” Service Note (SNAW3049) is focused on the password change details for both the Advantage Workstation product line and the AW Server product line. Refer to it for your information on SIMS Content Viewer.



A.6.2 Passwords Change Procedure

Refer to the AW Server 3.2 Installation and Service Manual, Job Card IST006 - Changing the Passwords for the detailed procedure.

A.6.3 Changing the passwords with FFA

The FFA users have the capability to update the passwords from the GE Backoffice for the systems remotely connected with Insite or RSvP.

NOTE

Once changed, the passwords may not be synchronized immediately with the customer system.

A.6.3.1 Changing the passwords in Insite

The system passwords can be updated from the GE Backoffice.

1. Remotely through FFA, display the **Re-Checkout** panel.

Connection Information (NETWORK)	
IP Connection Information	
Local IP Address	3.249.70.226
Network Address Translation IP	10.99.93.48
SPA Id	null
Comments	SYSTEMS ETHERNET PORT
Passwords	
Login ID	Password
sdc	odw2.0
root	Tod&bu
insite	Gelaw-G08
<input type="button" value="Update Passwords"/>	
Language	
Language options could not be determined. Using checkout will set the language as English.	

2. In the **Checkout** tab enter the new passwords and click on **Update Passwords**.
3. Proceed with **Post Checkout**.

A.6.3.2 Changing the passwords in RSvP

The passwords for *root* and *filetransfer* system users/accounts and the password for *service* can be updated from the GE Backoffice.

1. Remotely through FFA, display the **System Password Vault** panel.

Showing 3 configured accounts for System ID AWBUCLAB162

#	App Name	Username	Password	Last Updated	Updated By	Actions
1	ea3	service	●●●●●●●●	Feb-17-2021 12:02:58	AGENT	Change Password
2	sftp	filetransfer	●●●●●●●●	Mar-14-2021 02:00:02	AGENT	Change Password
3	ssh	root	hebhOtYvPOGG0qY LcOgP@ktEpb	Mar-14-2021 02:00:09	AGENT	Change Password

Enter New Password

 217 characters left

2. Select **Change Password** and enter the new password.
3. Select **Update Password** to change the password.

A.7 Setting Date and Time

This section provides instructions for remotely setting the AW Server's date and time using several methods: Service Tools Time Settings or Command Lines from the Terminal. The Service Tools Time Settings menu is the preferred solution to configure date and time after the first install as it provides a graphical interface to configure the Date and Time settings. For troubleshooting purposes, command Lines can be used from a terminal to perform Date and Time configuration.

NOTE

YaST is not available in AW Server 3.2. If you need a graphical user interface, use the Service Tools Time Settings menu.

A.7.1 Synchronization

There is NO TIME SYNCHRONIZATION between the AW Server and the clients. The following procedures set the AW Server clocks only.

It is recommended that the AW Server and clients use the same NTP server for synchronization.

NOTE

Configuring the NTP protocol on AWServers is mandatory for the management of a cluster of AWServers.

NOTE

For a virtual AW Server, it is the responsibility of the customer (IT Admin) to correctly configure the Hypervisor Date and Time. For VMware hypervisor, if VMware Tools are installed, it will automatically synchronize its date and time settings with the hypervisor by default.

Refer also to [2.3.5 Time Settings \(NTP\) on page 57](#).

A.7.2 Configuration with Service Tools Time Settings

The web-based Service Tools provide a menu to configure Time Settings. To access this menu:

- in an Internet browser, connect to the Service Tools by entering the IP address of the AW Server (e.g. <http://10.0.0.12>)
- Select **Launch** then login as service or admin user.

- Select **Initial Configuration > Time Settings**
- In the **Date/Time** tab
- select the appropriate Region and Timezone from the drop-down lists and hit **<Apply>**.
- A message "Success" should display next to the Cancel button.
- Enter the Date (format DD/MM/YYYY) and the Time (format HH:MM:SS) and hit **<Apply>**.
- A message "Success" should display next to the Cancel button.

The changes in Date and Time Settings have been taken into account. There is no need to reboot the Server to apply them. Also, after a reboot, the date and time settings that you configured are kept.

A.7.3 Configuration with Command lines from the terminal

Terminal enables to configure the AW Server using command lines.

Terminal can be access locally using the Server KVM. use the keyboard to enter command lines.

Terminal can be accessed remotely by an ssh client (e.g. putty). Alternatively, terminal can be accessed remotely from the AWS Service Tools. A description of Terminal is provided in the Service Tools section of this manual.

The Terminal allows multiple connections.

A.7.3.1 Server Clocks

The server has two separate clocks, a hardware clock and a system clock. This procedure provides instructions for setting both the hardware clock and the system clock. through command lines.

- **Hardware clock (rtc)**

The hardware clock, also known as the "rtc" or real-time clock, is a clock circuit that is part of the server's internal hardware. It keeps time continuously using a quartz-crystal timebase. A battery keeps the clock running when the server is powered down. The hardware clock is typically used only to set the system clock when the server boots up.

- **System clock**

The system clock is a software clock that runs only while the system is powered up. This is the clock used by most Linux applications. Typically, each time the server is powered up or rebooted, the system clock sets itself by reading the hardware clock time.

NOTE

Setting only the system clock will **not** maintain the changed date and time after a reboot. To permanently change the time (i.e., to maintain the time change after the server is rebooted), you must also transfer the new date and time from the Linux system clock to the hardware clock.

NOTE

The server's hardware clock should always be set to UTC (Universal Time, formerly known as Greenwich Mean Time). Typically, the system clock is set to display local time. For example, if the server is located in Chicago, Illinois, the system clock is set to the Central Time zone.

A.7.3.2 Changing the Time and Date using Terminal

Basically, the procedure is to use the "**date**" command to set the *system* clock, then use the "**hwclock**" command to set the *hardware* clock to the system clock. Detailed instructions are provided later in this appendix.

A.7.3.3 Start the Terminal Tool

Use any of the following methods to access the terminal: KVM access, ssh client (putty) or Service Tools>Tools>Terminal.

- At the "Login" prompt, type **root** then press **Enter**.
- At the "Password:" prompt, type the default password (unless it has been changed to something else – see [A.6 Password Change on page 484](#)), then press **Enter**.

NOTE

For security purposes, Terminal does not display any characters while you type the password.

You are now logged into the AW Server. You can send commands to the server via the command line interface as described in this section.

A.7.3.4 The "date" Command

The **date** command is used to display and set the time and date in the system clock.

NOTE

Setting the time using only the **date** command will **not** maintain the changed date and time after the server is rebooted. The **date** command sets only the Linux system clock, not the hardware clock. To permanently change the system time (i.e., to maintain the time change after the server is rebooted), you must also use the "**hwclock**" command to transfer the new date and time from the Linux system clock into the hardware clock. The "**hwclock**" command is described in this section.

A.7.3.5 The "hwclock" Command

The "**hwclock**" command displays the time and date from the hardware clock. It is also used (with specific command options) to set the hardware clock time to the system clock time.

A.7.3.6 How to set the System Clock Time using Terminal

At the Terminal prompt, type **date** to display the current system clock time and date. If the time and/or date need to be changed, enter the new time and date as follows:

- Enter **date MMDDhhmmYYYY** to set the current system date/time, where
 - MM = month (two digits)
 - DD = day of month (two digits)
 - hh = hour (two digits, in 24-hour format)
 - mm = minute (two digits)
 - YYYY = year (four digits) (optional)

For example, entering "**date 07151352**" (without the quotation marks) sets the date to July 15 and the time to 13:52:00. (See the figures)

NOTE

Use the "**date**" command to change both the date and the time of the system clock.

Figure A-6 CHANGING THE SERVER DATE USING TERMINAL

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Tue Jul 15 10:10:39 2008 from localhost
aws-59:~ # date
Tue Jul 15 10:44:56 CDT 2008
aws-59:~ # date 07151352
```

Figure A-7 ENTERING THE NEW TIME AND DATE

```
aws-59:~ # date 07151352
          ^   ^   ^   ^
          month date hour minute
```

A.7.3.7 Setting the Year using Terminal

The previous step shows how to set the date and time without changing the year. If you also want to change the year, append the four-digit year onto the end of the date without a space. For the example shown in the figure, the command would be:

"date 071513192008" (without the quotation marks), which sets the time and date to 13:19, July 15, 2008.

Figure A-8 SYNTAX FOR ENTERING DATE WITH YEAR

```
aws-59:~ # date 071513192008
          ^   ^   ^   ^
          month date hour minute
          year (optional)
```

A.7.3.8 Setting the Hardware Clock using Terminal

After you have correctly set the system clock date and time, you must set the hardware clock ("rtc", or real-time clock) to the system clock time in order to keep the new time setting after the server is rebooted. If you don't do this, the new time setting will be lost when the server is powered down or rebooted.

The hardware clock is not set directly. It is set by first setting the system clock to the correct time, then setting the hardware clock to the current system time. This is done using the "**hwclock**" command as described in the following paragraphs.

A.7.3.8.1 Using the "hwclock" command

- At the command line prompt, type in "**hwclock --utc --systohc**", then <ENTER>.

This will force the hardware clock to set itself to the system clock time.

NOTE

Be sure to put two dashes before **--utc** and before **--systohc**.

A.7.3.9 Changing the System Clock's Time Zone: Do Not Use Terminal

Do not use Terminal alone to change the system clock time zone. Instead, use the procedure "Configuration with Service Tools Time Settings" or "Configuration with AWS scripts"

NOTE

Do not change the hardware clock's time zone. It must remain set to UTC (Universal Time). If you need to change the time zone, change only the system clock's time zone.

A.7.4 Configuration with AWS scripts

The advantage of using AWS scripts to change the time and date, rather than using the command-line interface directly, is that AWS scripts provides interactive prompts.

From the command line, type:

```
sh /root/sys-times-conf <Enter>
```

Follow the instructions displayed to configure the Time Zone, Date and Time.

- Enter the number corresponding to your continent/ocean, then hit <Enter> (e.g. **8** for Europe, **3** for Antarctica...)

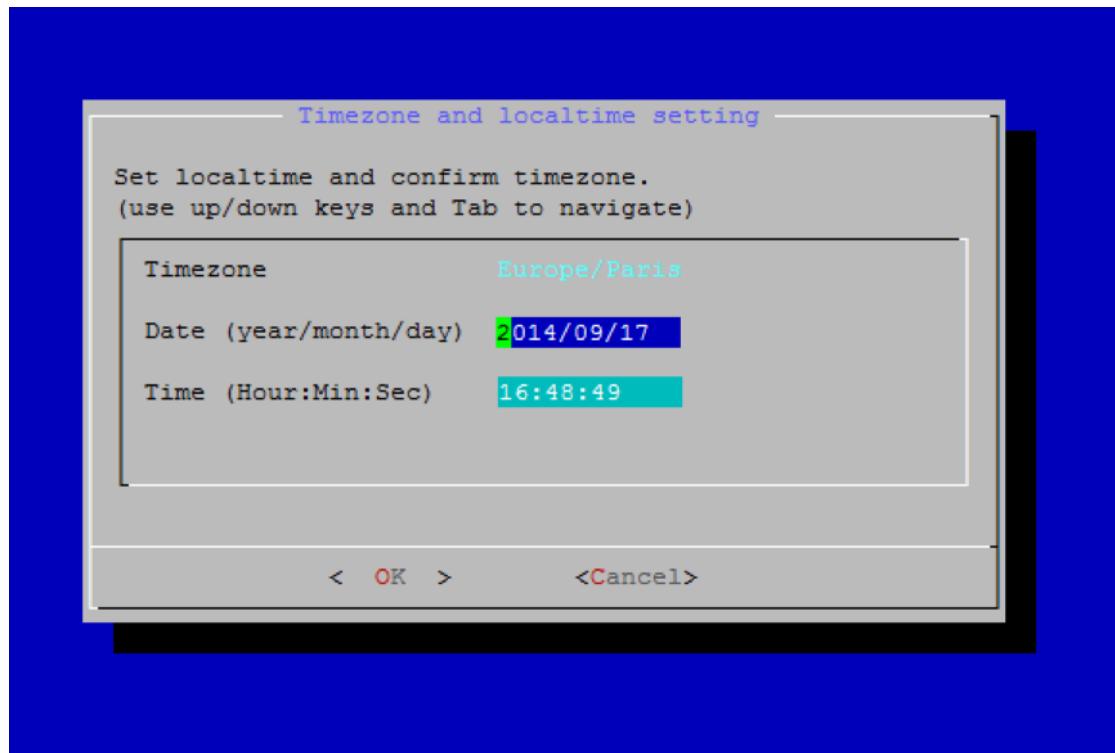
```
Timezone selection - confirmation at last in the localtime dialog.

Select a continent or ocean
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) Etc - Specify the time zone using the Posix TZ format.
#? 8
```

- A list of country displays for the continent/ocean that you selected.. Enter the number corresponding to your country, then hit <Enter> (e.g. **16** for France, **41** for San Marino...)

5) Austria	22) Ireland	39) Romania
6) Belarus	23) Isle of Man	40) Russia
7) Belgium	24) Italy	41) San Marino
8) Bosnia & Herzegovina	25) Jersey	42) Serbia
9) Britain (UK)	26) Latvia	43) Slovakia
10) Bulgaria	27) Liechtenstein	44) Slovenia
11) Croatia	28) Lithuania	45) Spain
12) Czech Republic	29) Luxembourg	46) Sweden
13) Denmark	30) Macedonia	47) Switzerland
14) Estonia	31) Malta	48) Turkey
15) Finland	32) Moldova	49) Ukraine
16) France	33) Monaco	50) Vatican City
17) Germany	34) Montenegro	
#? 16		

- A date & time dialog box opens. Enter the correct date using the format YYYY/MM/DD, then use the up/down arrow to select the time field and enter the time using the format HH:MM:SS
- When done, press the **<Tab>** key to select **<OK>** then hit **<Enter>**. The date displays in the command line, in a format similar to `Wed Sep 17 17:02:59 CEST 2014`



A.8 Command Line Tools

The following is a list of command line tools that may be helpful in managing AW Server software remotely. This list does not contain standard UNIX/Linux commands, as it is expected that the Field Engineer servicing AW Server is proficient in UNIX/Linux commands.

NOTICE

Use these commands only when the ServiceTools GUI is not available. Use these commands only if you have proficiency in UNIX/Linux.

Command	Arguments	Executed as	Purpose
/export/home/sdc/AIA/UFO/Filmer/bin_x86_64/start.test-PrintComm	--echo--list-queue[=user] --get-history[=user]--pause-queue--resume-queue--cancel-job=[reserved_space]	sdc	Test Filmer communication status and manage queue
/usr/share/ServiceTools/scripts/healthpage/restart_all.sh	none	root	Restarts all server processes in correct order. Note: This will disconnect any connected clients
/usr/share/Service-Tools_AWS/scripts/health-page/get_service_processor.sh	none	root	Returns the IP address for the service processor.
/usr/share/Service-Tools_AWS/scripts/health-page/get_raid_status.sh	none	root	Returns any RAID error messages in /var/log/messages
/usr/share/Service-Tools_AWS/scripts/iip/iip-serv_config.sh	enable disable	root	Enables / disable IIP, and telnet and ftp for IIP. Prior to executing this IIP gateway needs to be added to the .insiteInfo file.
/usr/share/ServiceTools_AWS/scripts/iip/iipserv_config.sh enable	enable disable	root	Enables telnet and ftp for IIP
cat /var/log/firewall	none	root	Displays IP addresses that have been blocked by the firewall
/usr/share/gehc_security/pnf/manager	see SERVER FIREWALL (PNF) section in service manual	root	see SERVER FIREWALL (PNF) section in service manual
licenseAdmin	-help to see options	sdc or gehc_security	Manage floating license server.Adding applications licenses must be performed as user "gehc_security" Adding license server license must be done as user "sdc"
/usr/share/awe/sweep/healthbase.sh	Creates a software & hardware sensor / RAID status report in /tmp/result	root	Overall Server Health SWEEP script.
shutdown -h 0		root	Graceful shutdown of the Server
halt		root	Quick shutdown of the Server
/opt/InSite/InSiteAgent/bin/AgentStatus.py	none	root	Display the RSvP Agent
/opt/InSite/InSiteAgent/bin/StopAgent.py	none	root	Stop the RSvP Agent
/opt/InSite/InSiteAgent/bin/StartAgent.py	none	root	Restore the RSvP Agent after it has been installed and configured
/opt/InSite/InSiteAgent/bin/RestartAgent.py	nonea	root	Restart the RSvP Agent after a configuration change

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

A.9 Definitions and Acronyms

Term	Definition
CTQ	Critical to Quality
CRS	Component Requirement Specification
PPP	Product Program Proposal
SRS	Software Requirements Specification
URS	User Requirements Summary
AWS	Advantage Workstation Server = AWE – Advantage Workstation Enterprise
AWE	Advantage Workstation Enterprise = AWS – Advantage Workstation Server
ST	Service Tool
CST	Client Service Tool
LKGC	Last Known Good Configuration
External Evaluation	Generic reference = either a TE and/ or an ME
ME	PRD External Evaluation phase – usually between M1 and M2 or M3
TE	Technical Evaluation phase – usually pre M1
FDR (1,2,3...)	Formal Design Review – New version of M1, M2, M3... program phase milestone designations
RFS	Request for Service
MTTI	Service metric to establish the Mean Time To Install (Installation Time)
MTTR	Service metric to establish the Mean Time To Repair (How long does it take to fix the average system failure)
MTBF	Service metric to establish the Mean Time Between Failures (How long does the system operate between failures – on average)
QMI	Quick Market Intelligence. QMI is a way for a large business to respond to issues, competitive intelligence, new ideas and other information as a small business would. Cross-functional team members share their insights on the issues being presented which should relate to at least one of the following areas: <ul style="list-style-type: none">• - Competition• - Pricing• - Quality Assurance• - Customer Satisfaction• - Lessons Learned
EOL	End Of Life (as it relates to product software & hardware)
IPA (IP Address)	Internet Protocol Address (network address)
NTP	Network Time Protocol
SP	Service Processor (iLO)
KVM	Keyboard, Video Display, and Mouse

Term	Definition
iLO	<p>Integrated Lights Out Manager – A dedicated internal service processor located on the motherboard of a server, a PCI card, or on the chassis of a blade server or telecommunications platform. It operates independently from the server's CPU and operating system (OS), even if the CPU or OS is locked up or otherwise inaccessible. Some leading service processor technologies include:</p> <ul style="list-style-type: none"> • Intelligent Platform Management Interface (IPMI) • HP Integrated Lights Out (iLO) • IBM® Remote Supervisor Adapter (RSA) • Dell Remote Assistant Card (DRAC)
IPMI	<p>Intelligent Platform Management Interface – defines a set of common interfaces to computer hardware and firmware, which system administrators can use to monitor system health and manage the system. IPMI operates independently of the OS and allows administrators to manage a system remotely even in the absence of the OS or the system software, or even if the monitored system is not powered on. IPMI can also function when the OS has started, and offers enhanced features when used with the system management software. IPMI gives only the structure and format of the interfaces as a standard, where the implementation may vary.</p>
SMASH	<p>Systems Management Architecture for Server Hardware (SMASH) is a suite of specifications that deliver industry standard protocols to increase productivity of the management of a data center. The SMASH Command Line Protocol (SM CLP) specification provides an intuitive interface to heterogeneous servers independent of machine state, operating system or OS state, system topology or access method. It is a standard method for local and remote management of server hardware using out-of-band communication.</p>
RAID	<p>Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks – a technology that employs the simultaneous use of two or more hard disk drives to achieve greater levels of performance, reliability, and/or larger data volume sizes.</p>
DAS	<p>Direct Attached Storage – this is the name used to reference the J4200 disk drive chassis used for Image storage in the AW Server system.</p>
Fail-over	<p>Is the capability to switch over automatically to a redundant or standby computer server, system, network, or disk drive upon failure. Failover happens without human intervention and generally without warning.</p>
OS	<p>Operating System – as in Linux, etc...</p>
EA3	<p>Enterprise Authentication Authorization Audit. EA3 is a component to manage authentication and authorization on GE Healthcare Products. It supports both local and enterprise authentication infrastructures. All HIPAA-related authentication / authorization events are logged by EA3 through the EAT component.</p>
EAT	<p>Enterprise Authentication Trail</p>
HIPAA	<p>"HIPAA" is an acronym for the Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amended the Internal Revenue Service Code of 1986 – requiring: Improved efficiency in healthcare delivery by standardizing electronic data interchange, and Protection of confidentiality and security of health data through setting and enforcing standards. The bottom line: sweeping changes in most healthcare transaction and administrative information systems.</p>
QA Tool	<p>This is a client tool being developed in the program to run on the client, and will snapshot the hardware, software, and performance characteristics of the client against the AWS required specifications.</p>
FE	<p>Field Engineer</p>
GIB	<p>Global Installed Base</p>

Term	Definition
SSH (ssh)	<p>Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two computers. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which sent information, notably passwords, in plaintext, making it possible to intercept. The Encryption SSH uses provides confidentiality and integrity of data over an insecure network, such as the Internet.</p> <p>To use SSH, the host computer must either have SSH internal support, or an SSH tool such as "putty" installed and operable. Most Windows® computers do not have SSH support built-in.</p> <p>By default, SSH is not enabled on the AWS server. The other mechanisms for command-line access are built-in to the AWS Service Tools, the SSH connectivity tool or the Terminal tool in FFA, and the iLO service processor interface.</p>
Ethereal	<p>Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In June 2006 the project was renamed from Ethereal due to trademark issues. The functionality Wireshark provides is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.</p>
UTC	<p>Coordinated Universal Time (UTC) In casual use, Greenwich Mean Time (GMT) is the same as UTC and UT1. Owing to the ambiguity of whether UTC or UT1 is meant, and because timekeeping laws usually refer to UTC, GMT is avoided in careful writing. Time zones around the world are expressed as positive or negative offsets from UTC. Local time is UTC plus the time zone offset for that location, plus an offset (typically +1) for daylight saving time, if in effect.</p>
ANTA	<p>The IHE ANTA Profile for the secure exchange of healthcare information and the auditing of events related to the access, production or modification of healthcare information.</p>
iptables	<p>iptables is the userspace command line program used to configure the Linux 2.4.x and 2.6.x IPv4 packet filtering ruleset. It is targeted towards system administrators. Since Network Address Translation is also configured from the packet filter ruleset, iptables is used for this, too. iptables requires a kernel that features the ip_tables packet filter.</p> <ul style="list-style-type: none"> • Main Features: • listing the contents of the packet filter ruleset • adding/removing/modifying rules in the packet filter ruleset • listing/zeroing per-rule counters of the packet filter ruleset
VM	<p>Virtual Machine. A simulated computer hardware / operating system on which other software can be hosted as if on the real (non-virtualized) hardware / operating stem.</p>

A.10 Command-Line Interface

A.10.1 Command-line Interface

Command line usage

Command lines can be used to configure the AW Server's network, timezone, date and time settings. These command lines sometimes provide a simple keyboard-controlled graphical interface for the user.

To use command line, it is required to have access to the server local KVM (keyboard, video display, and mouse). Alternatively, you can use the service processor virtual console. It is also possible to use an ssh client to access the AW Server Terminal.

From the server command-line LOGIN prompt, login as user **root**, and use the default password (unless it has been changed to something else – see [A.6 Password Change on page 484](#)).

NOTE

YaST is not available in AW Server 3.2.

A.10.2 Getting hardware network information

At the command prompt type: **ifconfig <Enter>**

The Unix command **ifconfig** serves to configure and control network interfaces from a command line interface (CLI). In this case it will show the "active" connected interface(s).

The **Hwaddr** information in the example ifconfig output below is the unique physical **MAC** (media access address) of the interface **eth0**.

NOTE

This is an example. Obtain the actual MAC address from the AW Server.

```
eth0 Link encap:Ethernet HWaddr 00:0F:20:CF:8B:42
inet addr:217.149.127.10 Bcast:217.149.127.63 Mask:255.255.255.192
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2472694671 errors:1 dropped:0 overruns:0 frame:0
      TX packets:44641779 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1761467179 (1679.8 Mb) TX bytes:2870928587 (2737.9 Mb)
      Interrupt:28
```

Record the Hwaddr data MAC address (in this example **HWaddr 00:0F:20:CF:8B:42**) for the AW Server being configured.

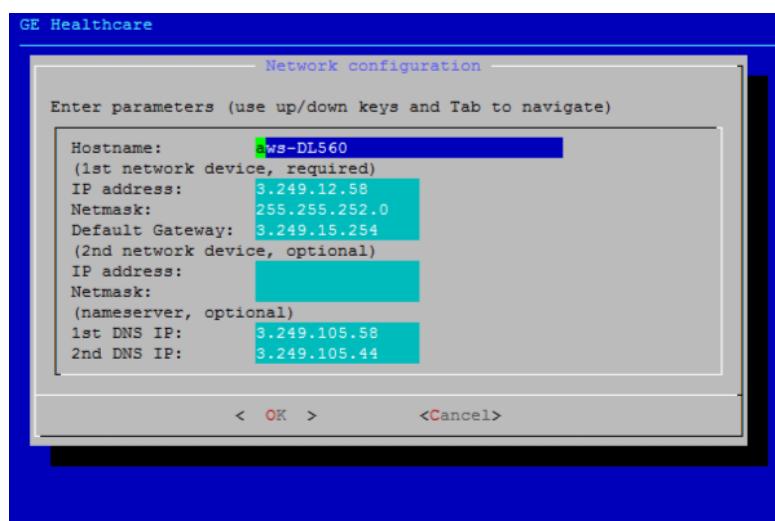
A.10.3 Configuring the network card using command lines (sys-net-conf)

In the AW Server terminal, type the following:

sh /root/sys-net-conf <Enter>

The following screen should display:

Figure A-9 SYS-NET-CONF COMMAND LINE



Enter the hostname for your AW Server, then use the arrow keys to move down to other parameters.

Mandatory parameters are: **Hostname, IP address, Netmask/Network Prefix** and **Default Gateway**.

Gateway. If one of these parameters is missing, the configuration will not be saved. Configuration of the second network card and configuration of the DNS are optional parameters.

If needed, you can also use tab to select **Cancel**, then press **<Enter>** to leave the menu without configuring the network.

Once done, hit **<Enter>** to apply the configuration.

Messages will display to indicate that changes are being applied. Network services will be stopped and restarted. Reboot is not needed to apply network changes.

To set the hostname, refer to the rules in the AW Server 3.2 Installation and Service Manual, Specific field - Characters rules and limitations.

NOTE

Physically, the first network device should be the first or left most network jack on the back of the server – eth0.

NOTE

ONLY ETH0 SHOULD BE CONNECTED AND CONFIGURED. THE SECOND ETHERNET DROP SHOULD BE LEFT DISCONNECTED – IP ADDRESS RESERVED FOR FUTURE USE.

NOTE

The command **system-config-network** provided by the OS shall not be used for network configuration as it does not correctly update all files.

A.11 HP ML350 server handling procedure

(Procedure to transport and unpack the HP ML350 server on-site, for one Field Engineer only). This procedure is applicable for both HP ML350 G6 and HP ML350p G8.

CAUTION



The HP ML350 server is heavy. It is above the 23kg / 50lbs safe weight lifting limit fixed by EHS directions for employee safety. If the handling has to be done by one person only, the following recommendations must be followed in order to reduce the risk for strains.



CAUTION



Safety shoes, eye protection and cut resistant gloves must be worn during cutting operations, and while handling the unit.



A.11.1 Unpacking procedure

Refer to the AW Server 3.2 Hardware Installation Manual.

A.11.2 Returning procedure

This section describes the return procedure of a defective unit after replacement by a FRU unit.

- Refer to [on page 498](#) to unpack and handle the FRU unit.
 - Re-use the packaging of the FRU unit to ship the defective unit back.
1. First of all, check if you can get help from some technical personal of the hospital, to unpack and move the unit to its final destination.
 2. Use the FE handcart or a customer hand dolly (see [on page 498](#)) to move the package to the room where the unit shall be installed.
 3. Tilt the defective unit on one of its sides and remove the 4 feet (if not done yet).
 4. Use the plastic bag to wrap the unit and place the 4 pieces of protection foam.



5. To ease the operation, you can secure the protection foam with tape before tilting the unit up.

6. Carefully tilt the unit up.



7. Insert the handcart under the unit and move it towards the packaging. make sure the packaging is placed against a wall so it does not tilt down. you can use tape to keep the packaging flaps open.



8. Roll the unit inside the packaging.



9. Tilt the packaging on its back, keeping the handcart in place.



10. Finally remove the handcart and insert the internal packaging, then close the packaging for shipment.

A.12 Old systems return process after upgrade

NOTE

Refer to the AW Server 3.2 Installation and Service Manual, Old hardware return procedure.

A.13 Filesystem Check

A.13.1 Filesystem Check feature description

The AW server is programmed to regularly run a Filesystem check upon reboot, in the following conditions:

- After a certain numbers of boot-up: typically around 30 - Note that this value can be different
 - After a certain elapsed time: typically every 6 months

These figures are available in the **System Configuration** section of the **HealthPage**:

When the mouse is pointed over the Mount count and Fsck values, it provides a short description about the meaning of the fields, and also mentions the rules for their coloring.

System Configuration	
System ID	AWBUCLAB237
Platform version	aws-3.2-3.2-1902.5-975c1d6d
Hostname / IP Address	bucaw70-237 / eth0: 3.249.70.237
DICOM Hostname / AET / Port	bucaw70-237 / bucaw70-237 / 4006
CPU (8)	Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Operating System	HELiOS release 6.10 (Carbon)
OS Version	6.10
Modality OS Version	AWS3.2_OS_5.0-1846.4-249f4bf8 [20181115]
UDI	(01)00840682102384(10)AWS3D2E003D2
REF	5719780
LOT	AWS3D2E003D2
Uptime	21 days
Region / Timezone	Europe / Paris
Memory Total / Free	65536 (MB) / 60865 (MB)
OS Disk Space Total / Free	41 (GB) / 25 (GB)
Image Disk Space Total / Free	94 (GB) / 76 (GB)
Backup Disk Space Total / Free	3 (GB) / 3 (GB)
Log Disk Space Total / Free	9 (GB) / 9 (GB)
Network Queue Status	In progress: 0 Pending: 0 Paused: 0 Failed: 0
Auto Delete (High / Low)	90 / 70
Delete option for worklist browser	Off
Image partition mount count (Current / Max.)	32/36
Image partition next file system check date	Sat
Certificate expiration date	Sat
Clam AV Antivirus Software status	Not
Machine type	VMware Virtual Platform ESXi 6.0
Install mode	server
DICOM AET (printing)	

NOTICE

The filesystem Check is necessary to preserve the AW Server's performances. Do not attempt to avoid it by cycling power off to the AW Server once the process has started. The process will start again from the beginning when turning on the server and booting up. Once the check is started there is no option to skip it. If the system is rebooted in the meanwhile, the filesystem can be damaged.

When FSCK is starting, the following messages are displayed as in the example below:

I.e: Waiting for /dev/sdc1 , no more events

Checking file systems

fsck x.xx.x (date)

```
/dev/sdb1 primary superblock features different from backup, check forced.  

/dev/sdb1 : xx/xxxxxx files (0.0x non-contiguous), xxxx/xxxxxxxx blocks  

/dev:sdb2 primary superblock features different from backup, check forced.  

/dev/sdb2 : .....
```

Filesystem check is launched for each partition of the AW Server, that is to say: System, Backup and Images. However, as the System and Backup partitions are much smaller than the Image partition (GB versus TB), fsck time will be hardly noticeable on those partitions. Note that there may also be a shift between fsck of System, Backup and Images partition, as during the OS load process, the system is rebooted several times, but the Image and backup partitions are not yet mounted, so the mount count is not "recorded" for them.

A.13.2 Filesystem check Side-effect "issue" description

The side-effect issue that can affect both the users or Service FE (during maintenance tasks such as upgrade, etc.) is that when rebooting the AW Server, the filesystem check may start unexpectedly, adding up to several hours to the bootup sequence time (depending on the number of images stored).

A.13.3 Solutions to minimize the impact

A.13.3.1 Upgrade to ext4 file system

The file system check is much faster on ext4 file systems than on ext3 file systems. Therefore, one solution to minimize the impact of fsck is to upgrade the filesystem of your server to ext4.

For all new installation of AW Server 3.2, ext4 is used by default. However IB systems which were running AW Server 2.0 are keeping their ext3 file system by default.

In order to upgrade the file system from ext3 to ext4, select erase image partition during AWS platform load.

NOTE

When erasing image partition, all image data are lost. Ensure that the data can be removed or back it up to a safe place before erasing the image partition.

Once you have selected erase image partition, the AWS platform installer will create a new image partition using the ext4 file system.

A.13.3.2 Check when the next Filesystem check is programmed

Refer to the **System configuration section of the HealthPage** (see [3.4.1 Understanding the HealthPage on page 154](#)).

NOTE

Alternate method to check when the next Filesystem check is programmed:

- Open a Terminal from the Service Tools, login as **root**.
- Identify the block device corresponding to the directory:

`df -h <Enter>`

- On a **HP DL580 hardware**, you should read:

`/dev/cciss/c0d0p2 xxx xxx xxx xx% /export/home1`

- Query the file system properties:

```
tune2fs -l /dev/cciss/c0d0p2 <Enter> (for HP DL580 high Tier hardware)
```

i.e:

```
Mount count: 26
Maximum mount count: 28
Last checked: Mon May 30 15:29:08 2010
Check interval: 15552000 (6 months)
Next check after: Sat Nov 29 14:29:08 2011
```

In our example, we can see that the Filesystem check is scheduled to start either in 2 boot-up (mount count is 26, and maximum count is 28) or at first boot-up after November 29th. Warn the IT Admin that the Filesystem Check should occur soon, so that they can force a check in advance over the next weekend for instance.

A.13.3.3 Minimize the impact for the users - Warn the IT Admin asap

In order to minimize the impact for users, the GEHC FE should warn the customer IT Admin about this feature and its side effects as soon as possible, and let them know the procedure for forcing the "fsck" launching at the best possible moment - i.e: before a weekend.

A.13.3.4 Minimize the impact for GEHC FE

NOTICE

Before performing a shutdown or reboot, refer to Chapter 2, [2.5.3 Shutdown / Reboot on page 96](#) for details of important precautions to take.

In the preceding example, we can see that the Filesystem check is scheduled to start either in 2 boot-up (mount count is 26, and maximum count is 28) or at first boot-up after November 29th.

This can be an issue for the GEHC FE if an on-site maintenance requiring a shutdown and reboot of the server several times is programmed in the coming weeks. To minimize the impact, proceed as follows:

Case 1: The Filesystem check can be launched in advance to GEHC FE on-site visit.

The mount count or the due date is getting close to filesystem check:

Contact the IT admin, and if they agree to launch in advance the Filesystem check (i.e: during the weekend for minimal impact for the users), remote log in to the system through FFA, open a Terminal (from the **Service Tools > Tools** menu) and launch the Filesystem check manually before the weekend prior to the GEHC FE on-site visit.This will avoid unexpected additional time to the bootup sequence and therefore to FE on-site time.

```
touch /forcefsck <Enter>
```

```
shutdown -r now <Enter>
```

These commands will reboot the system and enforce a filesystem check.

NOTE

After the filesystem check has completed and the AW server has rebooted, the result of the **tune2fs** command should indicate a `Mount count = 1` and a `Last checked date = [current date]`.

Case 2: The Filesystem check cannot be launched in advance to GEHC FE on-site visit.

The mount count or the due date is getting close and the IT admin is NOT able to launch in advance the

Filesystem check, with the minimal impact on the users, prior to GEHC FE on-site intervention for maintenance.

However it is not recommended to suppress the Filesystem check, useful for filesystem health, it is possible

to postpone the check to a later date if needed.

These commands shall be run by the GEHC FE, locally on the AW Server prior to proceed with the maintenance tasks, or remotely prior to go to the site.

NOTICE

The commands indicated below have to be executed directly on the KVM, or using the iLO. Do not use ssh or the Service Tools, because these two services will be stopped as part of the procedure. If you do use ssh or Service Tools, you will not be able to finish the procedure.

1. Open a root shell (Terminal: login as **root**).
2. Stop the services used by `/export/home1` and `/export/backup` (at least nuevo):

```
init 2 <Enter>
/etc/init.d/awsservicermi stop <Enter>
/etc/init.d/servicermi stop <Enter> (only from AWS gen2 release)
```

3. Umount `/export/home1`:

```
umount /export/home1 <Enter>
```

NOTE

The `/export/backup` filesystem is only 3GB size, so you can leave it mounted. The filesystem check when launching will not take long to complete on a 3GB partition.

NOTE

If an error reported that some processes are using the mount point, you can query the process id that uses it: `lsof | grep export/home1 <Enter>`

I.e: A terminal is open and connected to `/export/home1/sdc_image_pool/import` directory:

```
bash 21386 root cwd DIR 8,18 4096 189039103 /export/home1/
sdc_image_pool/import <Enter>
```

In this case close the terminal connected to the “import” directory or kill the process as below:`kill -9 21386 <Enter>`

and run the `umount` command again.

4. Then modify the Filesystem properties to postpone the Filesystem check:

Reminder: The condition for the automatic file system check routine to start at reboot is:

mount count \geq max mount count

OR

current date - last checked \geq check interval

You can adjust the following (suggestion is to set at least +10 for mount counter and give at least an extra week for the next automatic change)

- I.e: change check time interval to 200 days:

tune2fs -i 200d /dev/cciss/c0d0p2 <Enter> (HP server High tier)

tune2fs -i 200d /dev/cciss/c0d1p2 <Enter> (HP server low tier)

- I.e: change the max mount count to 40:

tune2fs -c 40 /dev/cciss/c0d0p2 <Enter> (HP server High tier)

tune2fs -c 40 /dev/cciss/c0d1p2 <Enter> (HP server low tier)

- Call the sync command to write out disk cache:

sync <Enter>

- Remount the file system manually:

mount /export/home1 <Enter>

The command should not report any problem, but a warning message is possible (the file system was not umounted clearly, suggest fsck!).

- Query the file system properties to make sure the modification has been done properly:

tune2fs -l /dev/cciss/c0d0p2 <Enter> (HP server High tier)

tune2fs -l /dev/cciss/c0d1p2 <Enter> (HP Low tier hardware)

- Perform reboot:

reboot <Enter>

NOTE

An alternative to using **tune2fs** commands is to use the following command as

root: touch /fastboot <Enter>

This will skip the fsck for the next reboot, and only for the next reboot. This means this command is only a very short term solution compared to **tune2fs**.

A.14 Launching AWS CLIENT on remote OLE laptop

- AWS Client software is installed on the Remote OLE laptop. Version of the client shall be compatible to the AW Server version you want to connect to.
- InSite (version prior to AW Server 3.2 Ext. 4.2) / RSvP (from version AW Server 3.2 Ext. 4.2) is properly configured and operational for the site.

The following procedure allows the Remote On-Line Engineer (OLE) to launch the AWS Client remotely on the OLE laptop, through FFA connectivity tools, using the FFA connectivity tools Port forwarding mechanism.

1. Remotely through FFA, start the Service Tools using the FFA connectivity tool, as described in [3.3.2 Accessing Service Tools from FFA on page 145](#).

The URL of the window is:

- For InSite connectivity:

https://<hostname>:<port number>/ServiceTools/ServiceTools.html

E.g: **https://g5zz3qf2e:9302/ServiceTools/ServiceTools.html**

- For RSvP connectivity:

https://127.0.0.1:<port number>

E.g: **https://127.0.0.1:10000**

2. Launch the AW Server Client and enter the following URL in the **Host** field:

- For InSite connectivity:

service://<hostname>:<port number>

E.g: **service://g5zz3qf2e:9304**

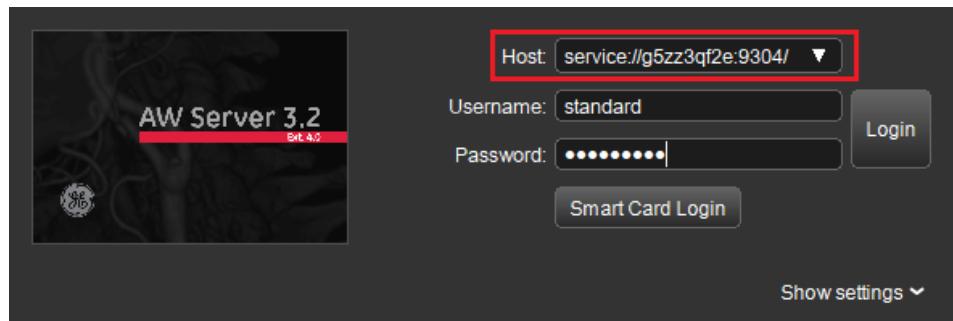
- For RSvP connectivity:

service://127.0.0.1:<port number>

E.g: **service://127.0.0.1:10000**

NOTE

The client login shall be done right after opening the connectivity tool in the FFA as the port forwarding link get outdated if not using it for a while. See below example for InSite connectivity:



3. Fill in the **Username** and **Password**, then login.

The AW Server Client starts on the remote OLE laptop.

A.15 BIOS / FIRMWARE upgrade

NOTE

Before proceeding to the Firmware upgrade, please check the version of the iLO (you can find it on the iLO homepage). If the version is lower than 1.20, please upgrade it following the procedure described in [A.15.2.1 Installing a server patch on page 510](#).

A.15.1 HP Servers Firmware & BIOS upgrade

The following procedure explains how to upgrade the Firmware by booting on a media. It is applicable to all the Hardware (Hight Tier, Low Tier or DAS).

A.15.1.1 Preparation

1. Connect to HP website

- To download HP Service Pack for ProLiant, go to HP website at

http://h17007.www1.hp.com/us/en/enterprise/servers/products/service_pack/spp/index.aspx.

- In the **Documentation** tab, read the latest Server Support Guide to check if your server is supported.
- In the **Download** tab, click on the link to download the Service Pack. Pay attention that the size of the file does not exceed the size of a DVD (4 GB) if you plan to install it locally.

Full ISO Image

[HP Service Pack for ProLiant \(3.94 GB\)](#)

MD5 Checksum: ede2f6c3cf3d2577e76d8f1c2818b826

- Click on **Obtain software**. A message prompts you to sign-in to access the download page.

HP Service Pack for ProLiant

Restricted download

The download you requested requires an active warranty, HP Care Pack or support agreement linked to your HP Support Center profile. Please [sign-in](#) so that we can determine your entitlement eligibility to access this download. For information on how warranties, HP Care Packs and support agreements enable access to selec

- Click on **Create an Account** if you connect for the first time. If you already have an account, click on **Sign-in** and go directly to 2.
- Click again on **Obtain Software**. You will be asked to link a warranty or HP Care Pack to your profile. Click on the highlighted link (see below).

The download you requested requires additional authorization. To access this download, please [link a warranty or HP Care Pack to your profile](#). You may also view [Help on how to link a warranty or HP Care | For information on how warranties, HP Care Packs and support agreements enable access to](#)

- To do so, click on **Link warranties** in the left panel, then enter the Product Serial Number and Product Number of your server(s).

* = Required field

Product serial number*	Product number*	Country/region of purchase*	Assign nickname:	Ownership type*
1. <input type="text"/>	<input type="text"/>	<input type="text"/> United States <input type="button"/>	<input type="text"/>	<input type="button"/> Single
2. <input type="text"/>	<input type="text"/>	<input type="text"/> United States <input type="button"/>	<input type="text"/>	<input type="button"/> Single

NOTE

The following table will help you locate the HP tag with the Serial Number and the Product Number.

Hardware	Tag location
HPE ProLiant DL360 Gen10 Server	Pull the slide-out identity tag attached to the server on the upper-left side of the front panel.
HPE ProLiant DL360 Gen9 Server	
HPE ProLiant DL560 Gen8 Server	
HPE ProLiant DL580 G7 Server	
HPE ProLiant ML350p Gen8 Server	Pull the slide-out identity tag attached to the server on the right side of the front panel.
HP ProLiant ML350 G6 Server	On top of the Server and also on the rear panel.
HP D3600 DAS	On the rear panel.
HP D2600 DAS	



- Make sure to select either "United States" or "France" as the **Country/region of purchase** and "Mutliple" as **Ownership Type**. Click on **Submit**, then on **Done**.
- Go back to the download page (use the link in 1) and Sign-in.

2. Create the media

- At the very bottom of the Download page, click on **Receive for Free**.

[Installation](#)[Receive for Free](#)

- Fill-in the form and click on **Next**. You will receive an e-mail to the address you entered in the form. Click on the link contained.
- On the **Electronic Download** page, the field Confirmation Number must be pre-populated (if not, enter the confirmation number contained in the e-mail). Enter your e-mail address and click on **Submit**.
- The **Software downloads and licenses** page opens. Select **Use Standard Download** and download the iso file (click on the first button).

Software		File Size	More Details	Download
Description				
HP Service Pack for ProLiant 2014.09.0_792934-001 (spp_2014.09.0-SPP2014090.2014_0827.10.iso)	3.94 GB	More Details	Download	
HP Service Pack for ProLiant 2014.09.0_md5sum (spp_2014.09.0-SPP2014090.2014_0827.10.iso.md5sum)	0.06 KB	More Details	Download	
Additional License Authorization	0.08 MB	More Details	Download	

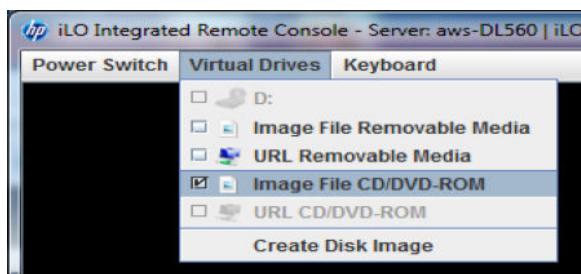
- You can either save this file on your PC to upgrade the Firmware remotely (go to [3](#)), or burn the iso file on a CDROM (using Roxio Creator or any CD/DVD creator software available) to upgrade it locally (go to [A.15.1.2 Firmware Upgrade on page 509](#)).

3. Boot on the media (remotely)

- Open an Internet Navigator on your Client PC or FE laptop to open the ILO Remote Console.
- Connect to the ILO website corresponding to your server. Go to `http://***IP Adress***/` (e.g. `https://3.249.12.59/index.html`). If you connect for the first time, use the following login credentials:

Local user name: **root**, Password: **changeme**. You will be asked to change the password.

- On the left panel of the page, select **Remote Console**, and click on the second button **Launch** to launch the Java Integrated Remote Console (Java IRC).
- When the console is open, press <Enter>. Log in as **root**.
- In the **Virtual Drives** menu, click on **Image File CD/DVD ROM** and select the iso file on your PC.



- In the Remote Console, enter **reboot** to reboot the server. It will boot on the Image file.
- Go directly to [A.15.1.2 Firmware Upgrade on page 509](#).

4. Boot on the media (locally)

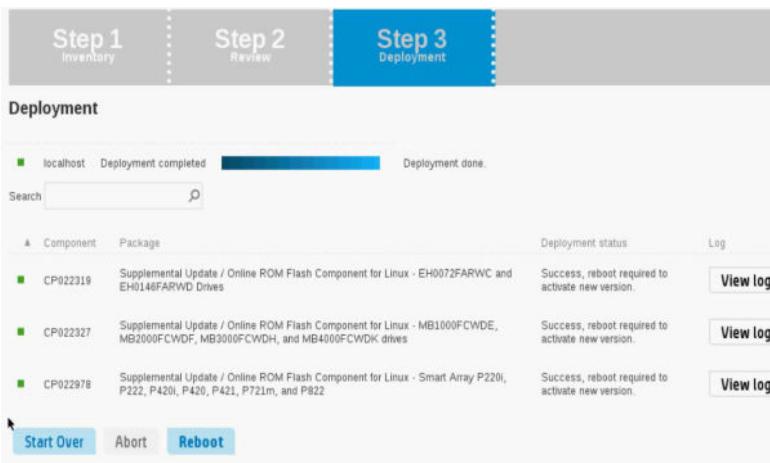
- Insert the CDROM into the Server disk drive or an external disk drive.
- Reboot the server. The server will boot on the media. (Attempting boot from CDROM). Note that the reboot can take up to several minutes.

A.15.1.2 Firmware Upgrade

- Select **Interactive Firmware Update Version 2014.06.0** and press <Enter>.



- Wait until the DVD is loaded (~5 minutes).
- Select the preferred language and accept the End User Agreement. Click on **Next**.
- Click on the left icon (**Firmware Update**).
- Wait while the following message is displayed: 'Please wait, loading HP SUM' (~10minutes).
- The Step 1 (Inventory) fills the content of the Proliant baseline and the content of the localhost.
- Click on **Next** to move to Step 2
- The Step 2 (Review) is displayed. Check the components that will be updated (all the necessary Firmware are selected by default) and make sure that the desired upgrade is selected (i.e. If you need to upgrade the Network Card to version 2.11.20).
- Click on **Deploy**.
- The Step 3 (Deployment) is displayed. The waiting time depends on the number of packages that will be deployed.
- The components successfully deployed are indicated with a green box and the column Deployment status displays 'Success'.



- Click on **Reboot** and acknowledge confirmation.
- Extract the CDROM from the disk drive while the server is booting. The Firmware/BIOS of all HW components is now updated.
- Once the Firmware have been upgraded, you need to check that the BIOS settings have not been modified
- The Hyperthreading must be disabled. Refer to the AW Server 3.2 Hardware Installation Manual, Configuring the Processor Hyperthreading.
- HP Power Profile must be set to Maximum Performance. Refer to AW Server 3.2 Hardware Installation Manual, Checking the BIOS Parameters Setup.

A.15.2 HP Servers Firmware & BIOS upgrade / patch installation

The following is the high level procedure to download patches from the HP download center, and install them on your AW Server.

A.15.2.1 Installing a server patch

1. From a client PC or FE laptop, open an Internet Navigator and connect to the HP Web site.
2. Download the required patch to your PC desktop.
3. FTP the patch (or use a USB disk or key) from the PC to the AW Server in the /tmp directory.
4. You may need to set the PNF firewall of the AW Server to off in order to authorize the transfer. At the KVM or remotely, type:
 - From AW Server 3.2 Ext. 4.0:
`systemctl stop pnf <Enter>`
 - For AW Server 3.2 Ext. 3.4 and previous versions:
`service pnf off <Enter>`
5. Login as **root** or remotely open a Terminal (from the **Service Tools > Tools**) and login as **root**.
6. Change dir to /tmp directory:
`cd /tmp <Enter>`
7. Change mode to give "execute" permissions:
`chmod 777 [patch_name].exe <Enter>`
(I.e: `chmod 777 SP53731.exe <Enter>`)
8. Execute the patch:
`[patch_name].exe <Enter>`
(I.e: `SP53731.exe <Enter>`)
9. Set the PNF firewall back to on:
 - From AW Server 3.2 Ext. 4.0:
`systemctl start pnf <Enter>`
 - For AW Server 3.2 Ext. 3.4 and previous versions:
`iptables -F <Enter>`
`service pnf on <Enter>`
10. Depending on the patch content, you may be given instructions to reboot the AW Server. If so, reboot then check that the system is operating properly.

A.15.2.2 iLO Firmware upgrade

NOTE

For the iLO Service Processor upgrade procedure, refer to the following sections:

- HPE ProLiant DL360 Gen10 Server: [2.6.3.2 iLO 5 Web Interface on page 102](#)
- HPE ProLiant DL360 Gen9 Server, HPE ProLiant DL560 Gen8 Server or HPE ProLiant ML350p Gen8 Server: [2.6.4.2 iLO 4 Web Interface on page 107](#)

- HPE ProLiant DL580 G7 Server: [2.6.5.2 iLO 3 Web Interface on page 113](#)
- HP ProLiant ML350 G6 Server: [2.6.6.2 iLO 2 Web Interface on page 118](#)

A.16 HP DL580/DL560/DL360 Handling Procedure

Refer to the Appendices of the AW Server 3.2 Hardware Installation Manual.

A.17 Secure Media Destruction Procedure

When you install software upgrades on a system, it is a Best Practice to destroy the installation media corresponding to previously installed versions. This reduces the risk that obsolete versions (which may contain software with safety or other issues) could be re-installed.

- Break all DVDs/CDs from the installation kit for the previous version.
- Delete any corresponding ISO files that you may have stored on your GE laptop or other storage devices.
- Use the Version Management tool to Remove the old package from the Server.
- Retain installation media only for currently installed versions of software.

If you need to reinstall an old version of software (perform a downgrade) at a later date on any given system, please contact your OLC for details of how to obtain it.

A.18 Application Profiles for AW Server

Refer to the AW Server 3.2 Installation and Service Manual, Job Card IST009 - External Application(s) Installation for the list of Applications currently supported with the AW Server 3.2 release.

A.19 Re-configuring Corrupted Serial Number

The Serial Number of a server Hardware in the BIOS and the OS should always match the Serial Number indicated on the label stuck on the Hardware. In some cases, the Serial Number in the BIOS is empty or corrupted.

The procedure below applies to HPE ProLiant DL560 Gen8 Server, HPE ProLiant DL580 G7 Server, HPE ProLiant ML350p Gen8 Server and HP ProLiant ML350 G6 Server as these hardwares share the same configuration utility for BIOS. This procedure is intended to configure Serial Number in the BIOS to match the Serial Number on the labels.

1. Identify the Serial Number indicated on the label stuck on the server (e.g. top of rear side for ML350p G8)
2. Reboot the server and type **<F9>** to enter the BIOS Setup utility. Refer to [2.5.3 Shutdown / Reboot on page 96](#).
3. Select **Advanced Options** by pressing **<Enter>**.
4. Select **Service Options** by pressing **<Enter>**.
5. Select **Serial Number** by pressing **<Enter>**.
6. Confirm the warning message by pressing **<Enter>**.
7. Change the Serial Number value to match the Serial Number stuck on the chassis, then press **<Enter>**.
8. Press **<Esc>** three times and press on **<F10>** to confirm Exit.

The procedure below applies to the HPE ProLiant DL360 Gen10 Server and the HPE ProLiant DL360 Gen9 Server.

For more details, refer to the AW Server 3.2 Hardware Installation Manual, Job Card IST006 - HPE ProLiant DL360 Gen10 Server Installation Steps (for HPE ProLiant DL360 Gen10 Server) or Job Card IST005 - HPE ProLiant DL360 Gen9 Server Installation Steps (for HPE ProLiant DL360 Gen9 Server).

1. Identify the Serial Number indicated on the label stuck on the server.
2. Reboot the server and type <F9> to enter the System Utilities menu.
3. Select **System Configuration** and press <Enter>
4. Type in the Administrator password when prompted (if applicable)
5. Select **BIOS/Platform Configuration (RBSU)** and press <Enter>
6. Select **Advanced Options** and press <Enter>
7. Select **Advanced System ROM Options** and press <Enter>
8. Select **Serial Number** and press <Enter>
9. Confirm the warning message by pressing <Enter>
10. Change the Serial Number value to match the Serial Number stuck on the chassis, then press <Enter>
11. When done, press <Esc> to return to the *BIOS/Platform Configuration (RBSU)* main menu.
12. Exit the *System Utilities* menu.

A.20 Sun High Tier X4450 returning Procedure

A.20.1 Foreword

The following is the procedure to safely return the Sun X4450 server in case of hardware upgrade to an HP server.

CAUTION



The Sun X4450 servers weigh approximately 25kg (56 pounds). This is above the safe weight lifting limit fixed by EHS directions for employee safety. Therefore, this procedure must be performed by 2 FEs, or 1 FE equipped with a Genie Lift or equivalent device.(The Genie Lift is orderable as Part number 5329416). Also adhere to the following Best Practices in order to reduce the risk for strains.



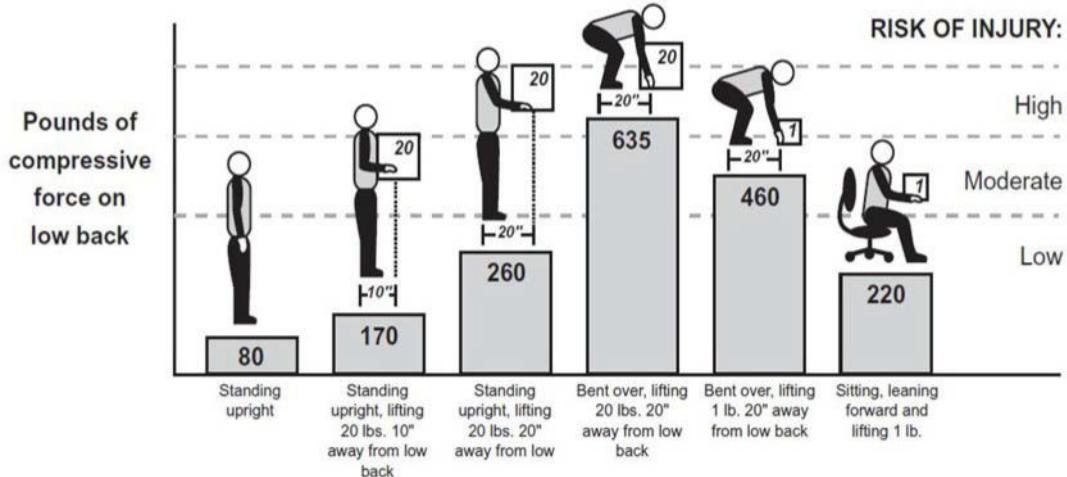
CAUTION



Safety shoes, eye protection and cut resistant gloves must be worn during cutting operations, and while handling the unit.

Your lifting posture affects your risk of injury: The weight of the objects you lift is an important factor in determining your risk of injury, and you will want to be especially careful when lifting heavy items such as storage boxes full of files and cases of copy paper.

However, weight is not the only thing that determines your risk of injury. The figure below shows the effect that posture can have when combined with lifting different size loads:



Force estimates based on the Michigan 2-D Static Strength Model

Position	Standing upright	Standing upright	Standing upright	Bent over	Bent over	Sitting and leaning fwd
Weight lifted lifting position	-	20 lbs / 9 kg 10" / 25.4cm	20 lbs / 9 kg 20" / 50.8cm	20 lbs / 9 kg 20" / 50.8cm	1 lb / 0.45 kg 20" / 50.8cm	1 lb / 0.45 kg -
Pounds/Kilograms of compressive force on low back	80 lbs 36 kg	170 lbs 76.5 kg	260 lbs 117 kg	635 lbs 285.7 kg	460 lbs 207 kg	220 lbs 99 kg
Risk of Injury	Moderate/low	Moderate	Moderate/high	High	High	Moderate

A.20.2 Returning procedure

In case of hardware upgrade of a Sun Server to an HP server, once all data is transferred to the new server, follow the steps below to return the old Sun Server Hardware:

- Prepare the package of the new server hardware, as it will be used to return the old server hardware. Ensure the package is empty except for the protective foam.
- If not done yet, remove the Sun Hardware from the server rack:
- Disconnect all the cables and power cords from the server.
- Extend the server to the maintenance position
- Press the metal lever that is located on the inner side of the rail to disconnect the cable management arm (CMA) from the rail assembly. The CMA is still attached to the cabinet, but the server chassis is now disconnected from the CMA
- From the front of the server, pull the release tabs forward and pull the server forward until it is free of the rack rails (a release tab is located on each rail)
- Set the server in the packaging you prepared. **Two people are needed for this step.** You might have to cut the protective foam from the HP package in order to fit the Sun server.
- Close the package with appropriate adhesive tape.

A.21 Installing/renewing an AW Server external CA signed certificate

By default, the AW Server is delivered with a self-signed certificate. This section describes how to install/renew an AW Server certificate signed by an external certificate authority.

AW Server certificate requirements:

- Shall contain only the public certificate of the AW Server signed by a CA.
- Supports the X.509 Linux based encoding scheme (extensions *.pem*, *.crt*, *.cer*).
- Does not support the *DER* encoding scheme.
- Does not require CA certificate.

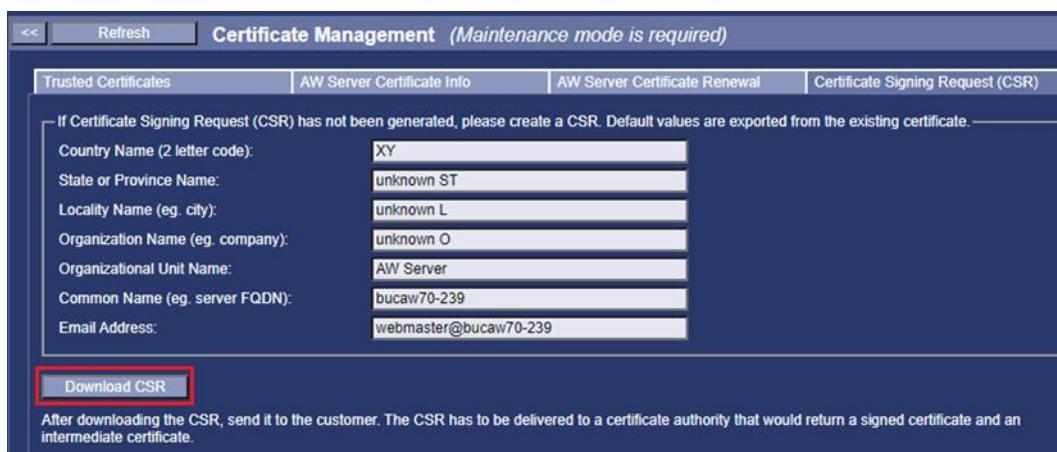
A.21.1 Installing/renewing an AW Server external CA signed certificate - from AW Server 3.2 Ext. 4.2

This section allows to generate an AW Server certificate signed by an external certificate authority, by:

- Generating a Certificate Signing Request (CSR).
- Exporting the AW Server certificate as CSR to be signed by external authority.
- Importing the trusted certificate to the AW Server.

1. Generating a Certificate Signing Request (CSR):

- a. From the Service Tools, select **Administrative > Configuration > Certificate Management**, and select the **Certificate Signing Request (CSR)** tab.



NOTE

The fields contain default values from the existing AW Server certificate. Review the fields with the customer IT admin before downloading the CSR.

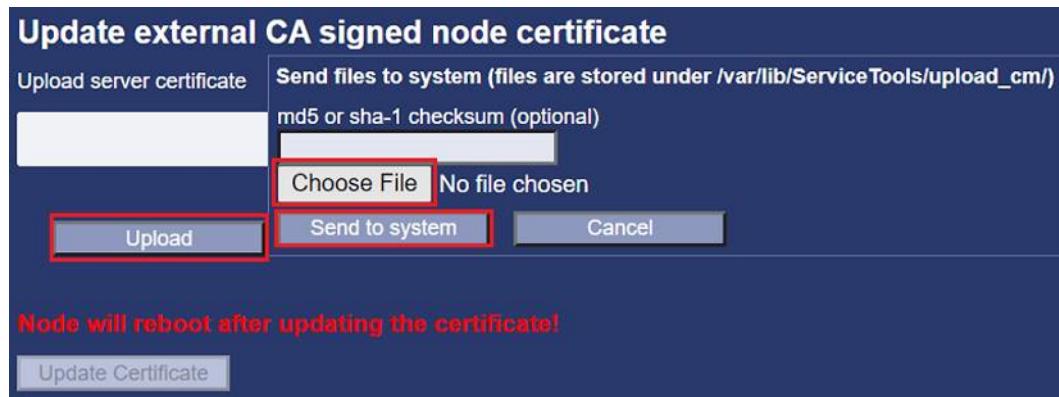
- b. Click on **Download** to download the CSR onto the PC.

A *server.csr* file is generated. It is a certificate not singed yet.

2. Exporting the AW Server certificate as CSR to be signed by external authority:

- a. Send the CSR to the customer and ask them to manage the signature with the external authority.

- b. In return, get a certificate signed by a certificate authority and copy it on your laptop or on an USB device.
3. Importing the trusted certificate to the AW Server:
- a. Select the **AW Server Certificate Renewal** tab.
 - b. In the *Update external CA signed node certificate* part of the page, click on **Upload**.



- c. Click on **Choose File** and select the certificate file stored on the PC or on an USB device.
- d. To upload the certificate file click on **Send to system**.

NOTE

The certificate file is uploaded into the `/var/lib/ServiceTools/upload_cm` location.

- e. When the file is loaded, click on **OK** in the pop-up window.

The certificate displays in the *Upload sever certificate* list.

NOTE

To delete an uploaded certificate, select the certificate in the *Upload server certificate* list and click on **Delete Uploaded**. Then acknowledge the popup that displays.

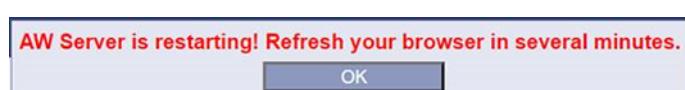
- f. Select the certificate in the *Upload server certificate* list and click on **Update Certificate**.
- g. In the warning message that displays, confirm the removal of the previous certificate and the installation of the new certificate.



- h. In the warning message that displays, confirm the reboot of the AW Server.



- i. Refresh the browser and login again into the Service Tools.



A.21.2 Installing/renewing an AW Server external CA signed certificate - for AW Server 3.2 Ext. 4.0 and older versions

This section does not describe how to generate a key pair or a certificate.

A certificate is composed of a **crt** and key files, **key** being the private key to the certificate and **crt** being the signed certificate (for instance **my_cert.crt** and **my_cert.key**). We assume that these two files are available.

NOTE

The common name (CN) of the certificate must contain the domain name of the server.

The server will have to be put in Maintenance Mode during this procedure. Plan the maintenance accordingly and warn the users.

A.21.2.1 Procedure

1. Copy the 3rd party certificate files (crt and key files) to the server:
 - In the **Service Tools > Tools > File Transfer**, select the **To system** tab. Browse to the location of the 3rd party certificate files stored on your laptop/PC, then select **Open**.
 - Select **Send to system**.
 - Alternatively, you can put the certificate on a USB stick and physically mount it on the AW Server system. The path to the USB stick should be similar to /dev/sdc1.
2. Access the command line of the AW Server:
 - directly on the server KVM (Keyboard Video Monitor)
 - In **Service Tools > Tools > Terminal**, select **New modal Terminal** button.
 - with putty, via SSH. Go to **Service Tools > Tools > Terminal** and put SSH to **on**. Then connect with putty to the AW Server IP address.
3. Backup the previous certificate file (the default self-signed certificate) and private key by executing the following command:

```
cp /etc/pki/tls/certs/server.crt /etc/pki/tls/certs/server.crt.old
<Enter>
```

```
cp /etc/pki/tls/private/server.key /etc/pki/tls/private/server.key.old
<Enter>
```

4. Add private key to the uploaded certificate file. In the command below, replace **my_cert.crt** and **my_cert.key** by the actual name of the certificate files.

```
cat /var/lib/ServiceTools/upload/my_cert.key >> \
/var/lib/ServiceTools/upload/my_cert.crt <Enter>
```

5. Copy the extended Certificate file to the right directory. In the command below, replace **my_cert.crt** by the actual name of the certificate file.

```
cp /var/lib/ServiceTools/upload/my_cert.crt \
/etc/pki/tls/certs/server.crt <Enter>
```

Overwrite current **server.crt** file.

6. Copy the uploaded private key file to the right directory. In the command below, replace **my_cert.key** by the actual name of the certificate file.

```
cp /var/lib/ServiceTools/upload/my_cert.key \
```

```
/etc/pki/tls/private/server.key <Enter>
```

Overwrite current server.key file.

7. For AW Server 3.2 Ext. 4.0 only, execute the command:

```
jki_mgmt -importServerKeypair <Enter>
```

8. Reboot the server.

NOTE

Ensure that the AW Server is in Maintenance Mode before doing this step.

```
reboot <Enter>
```

NOTE

After executing this procedure, the certificate expiration date displayed on the healthpage corresponds to the new certificate.

A.21.2.2 Revert procedure

1. Move the backup files back to their original locations with the following commands:

```
cd /etc/pki/tls/certs/ <Enter>
```

```
cp server.crt server.crt.new <Enter>
```

```
cp server.crt.old server.crt <Enter>
```

Overwrite current server.crt file.

```
cd /etc/pki/tls/private/ <Enter>
```

```
cp server.key server.key.new <Enter>
```

```
cp server.key.old server.key <Enter>
```

Overwrite current server.key file.

2. Apply the old certificate to the keystores and reboot the server:

```
jki_mgmt -importServerKeypair <Enter>
```

3. Reboot the server.

NOTE

Ensure that the AW Server is in Maintenance Mode before doing this step.

```
reboot <Enter>
```

A.22 Hardware Security

A.22.1 Hardware security - additional setup

Hardware security is essential to minimize the risks of software hacking.

We strongly recommend that you proceed to hardware BIOS lockup when done with the hardware configuration steps, and make sure that you have notified the IT admin of the site.

Refer to the following documents available on SIMS Content Viewer and Customer Documentation Portal:

- HPE ProLiant DL360 Gen10 Server Maintenance and Service Guide 869839-404
- HPE ProLiant DL360 Gen9 Server Maintenance and Service Guide 767928-008

- HP ProLiant DL560 Gen8 Server Maintenance and Service Guide 696743-005
- HP ProLiant DL580 G7 Server Maintenance and Service Guide 595655-005
- HPE ProLiant ML350p Gen8 Server Maintenance and Service Guide 661081-009
- HP ProLiant ML350 G6 Server Maintenance and Service Guide 513502-009

A.22.1.1 Pre-requisite

1. The Boot order should be set to boot from Hard disk first, in order to bypass the boot from CD/DVD or USB media.

Refer to the AW Server 3.2 Hardware Installation Manual, Changing the boot order for instructions.

2. A BIOS Administrator password should be setup.

Refer to the AW Server 3.2 Hardware Installation Manual, Setting up a BIOS administrator password for instructions.

A.22.1.2 HPE ProLiant DL360 Gen10 Server hardware security setup

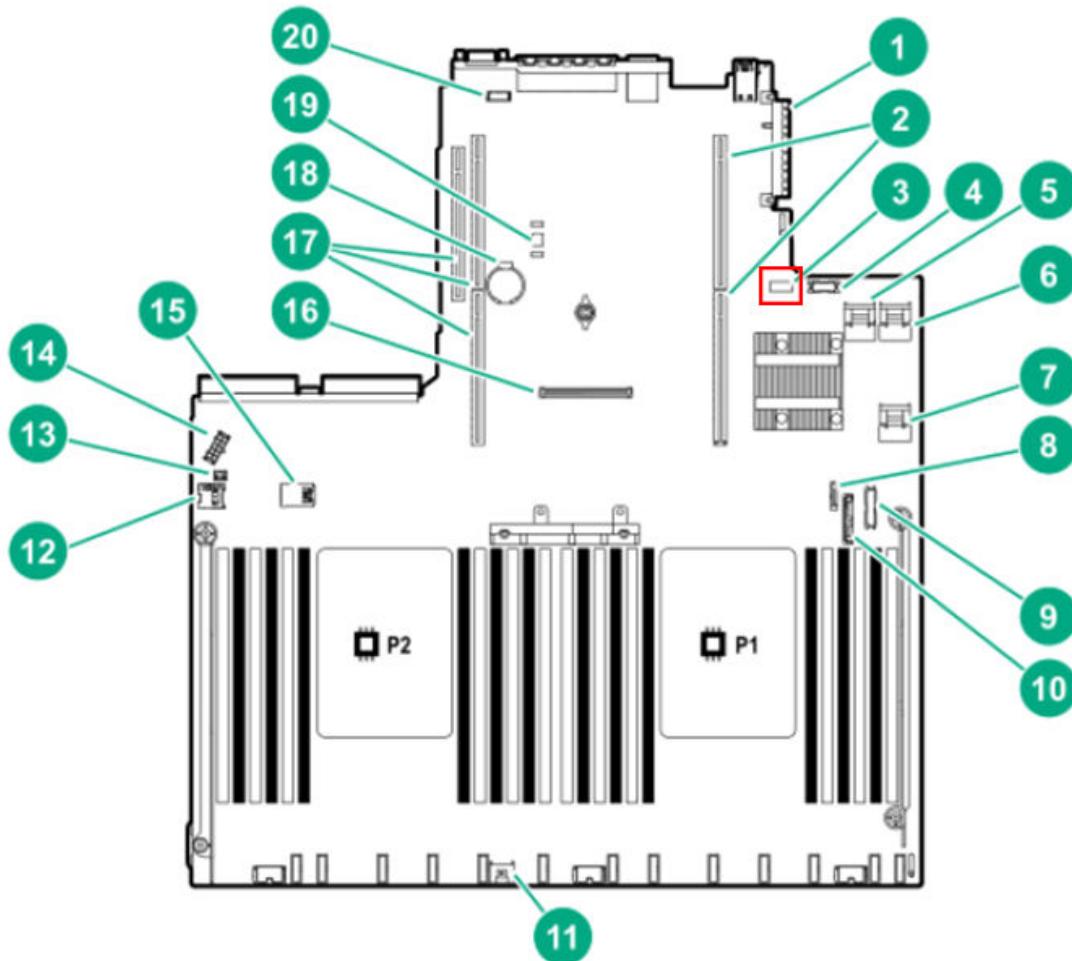
1. Shutdown the server, following the proper shutdown procedures (I.e: first, send a broadcast message if the server is in use).

Refer to the AW Server 3.2 Installation and Service Manual for instructions.

2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cable if its length is insufficient to allow the server extraction from the rack.

3. Extend the server and open the top access panel.

- Locate the System maintenance switch.



- Setup the System maintenance switch.

The system maintenance switch is a twelve-position switch that is used for system configuration. The default position for all switches is Off.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Reserved	Reserved
S3	Reserved	Reserved
S4	Reserved	Reserved
S5	Password protection override	Off = Power-on password is enabled. On = Power-on password is disabled.
S6	Invalidate configuration	Off = No function On = ROM reads system configuration as invalid.
S7 to S12	Reserved	Reserved

NOTE

There is no position to lock the system configuration.

- Close the cover of the server.
- Reconnect any disconnected cables.

8. Connect power supplies to the mains.
9. Reboot the server.

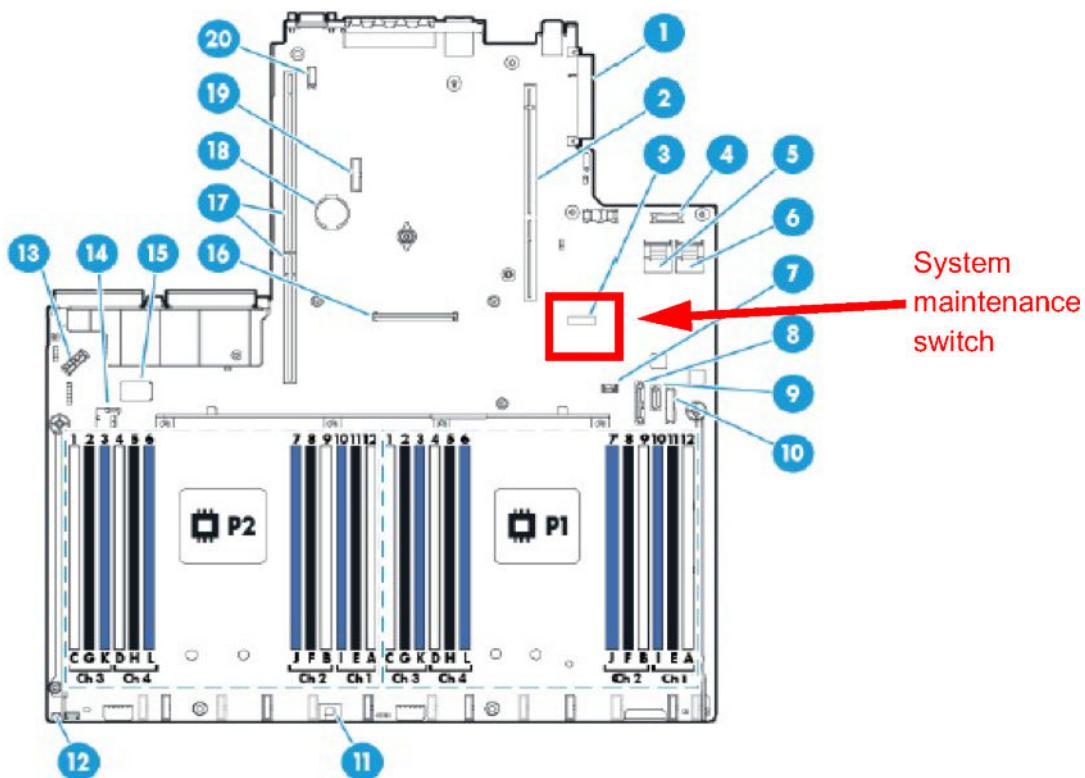
NOTE

In case the iLO password is lost or corrupted:

1. Power off the system.
2. Set the S1 switch to On.
3. Power on the system again.
4. Login to the iLO.
5. Set a new password.
6. Power off the server.
7. Set the S1 switch back to Off to enable iLO security.

A.22.1.3 HPE ProLiant DL360 Gen9 Server hardware security setup

1. Shutdown the server, following the proper shutdown procedures (I.e: first, send a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cable if its length is insufficient to allow the server extraction from the rack.
3. Extend the server and open the top access panel.
4. Locate the System maintenance switch.



5. Setup the System maintenance switch.

The system maintenance switch is a twelve-position switch that is used for system configuration. The default position for all switches is Off.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.
S3	Reserved	Reserved
S4	Reserved	Reserved
S5	Password protection override	Off = Power-on password is enabled. On = Power-on password is disabled.
S6	Invalidate configuration	Off = No function On = ROM reads system configuration as invalid.
S7	Default boot mode	Off = Set default boot mode to UEFI. On = Set default boot mode to legacy.
S8 to S12	Reserved	Reserved

To lock the system configuration, set the S2 switch of the System maintenance switch to On.

6. Close the cover of the server.
7. Reconnect any disconnected cables.
8. Connect power supplies to the mains.
9. Reboot the server.

To change the system configuration at a later time, refer to the procedure above to set back the S2 switch to Off, modify the configuration as necessary then set back the S2 switch to On.

NOTE

In case the iLO password is lost or corrupted:

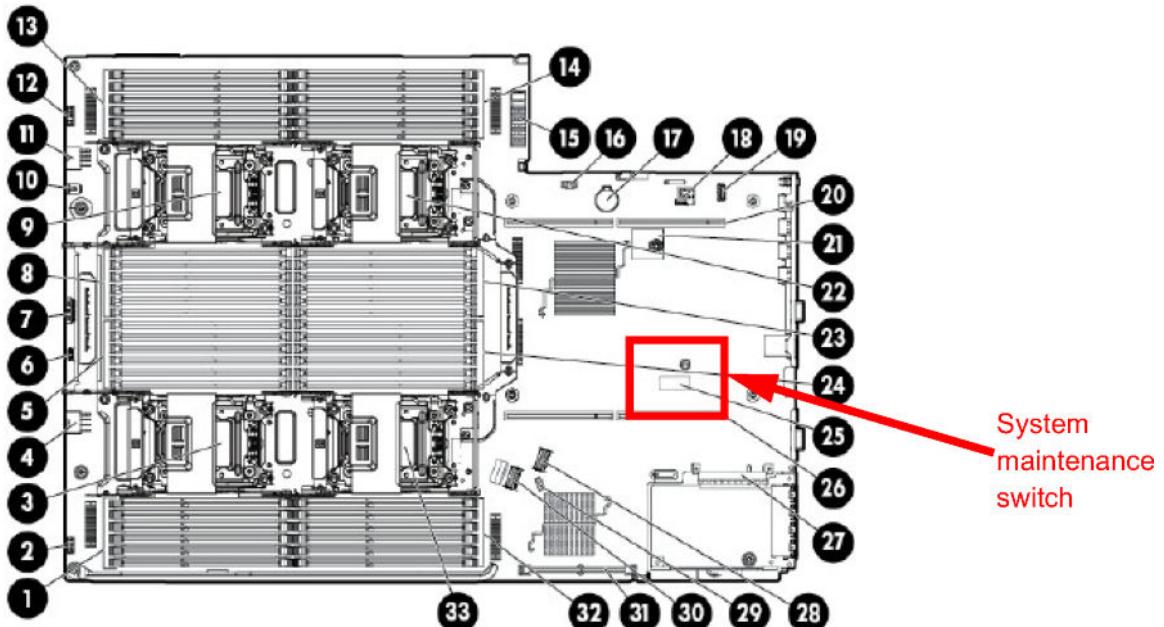
1. Power off the system.
2. Set the S1 switch to On.
3. Power on the system again.
4. Login to the iLO.
5. Set a new password.
6. Power off the server.
7. Set the S1 switch back to Off to enable iLO security.

A.22.1.4 HPE ProLiant DL560 Gen8 Server hardware security setup

Pre-requisite: The software is loaded on the server.

1. Shutdown the server, following the proper shutdown procedures (I.e: sending first a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cable if its length is insufficient to allow moving out the server.
3. Extend the server and open the top access panel.
4. Locate the System maintenance switch.

5. Setup the System maintenance switch.



System maintenance switch

The system maintenance switch is a twelve-position switch that is used for system configuration. The default position for all positions is **Off**.

- To lockup system configuration, once configuration has been setup to your needs, move the **S2** switch of the System maintenance switch to **On**. Then reconnect the power supplies to the mains and reboot the server.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.
S3	Reserved	Reserved
S4	Reserved	Reserved
S5	Password protection override	Off = Power-on password is enabled. On = Power-on password is disabled.
S6	Invalidate configuration	Off = Normal On = ROM reads system configuration as invalid.
S7 to S12	Reserved	Reserved

To change the system configuration at a later time, refer to the procedure above to set back the S2 switch to **Off**, modify the configuration as necessary then set back the S2 switch to **On**.

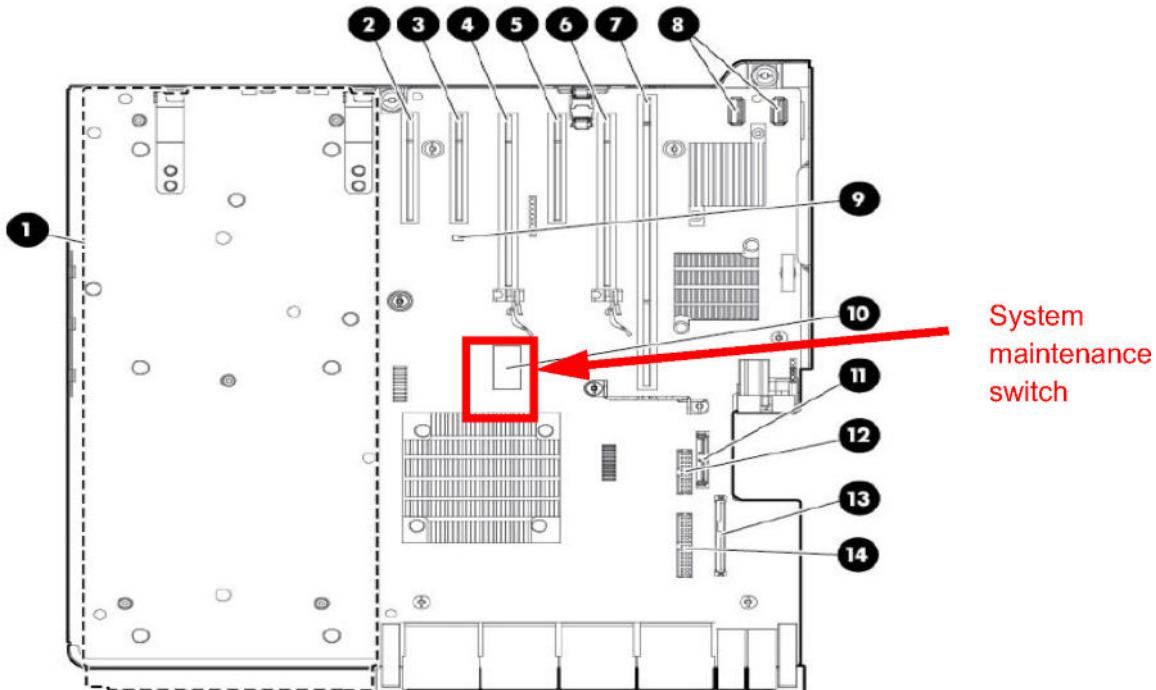
NOTE

S1 switch: In case the ILO password would be lost or corrupted, you should power off the system, set the S1 switch to **On**, power on the system again, login to the ILO, set a new password, then power off the server and set the S1 switch back to **Off** to enable ILO security.

A.22.1.5 HPE ProLiant DL580 G7 Server hardware security setup

Pre-requisite: The software is loaded on the server.

1. Shutdown the server, following the proper shutdown procedures (I.e: sending first a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cable if its length is insufficient to allow moving out the server.



3. Extend the server and open the top access panel.
4. Locate the System maintenance switch.
5. Setup the System maintenance switch.

System maintenance switch

The system maintenance switch (SW1) is an eight-position switch that is used for system configuration. The default position for all positions is **Off**.

- To lockup system configuration, once configuration has been setup to your needs, move the **S2** switch of the System maintenance switch to **On**. Then reconnect the power supplies to the mains and reboot the server.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.
S3	Reserved	Reserved
S4	Reserved	Reserved

Position	Description	Function
S5	Password protection override	Off = No function On = Clears power-on and administrator password(s)
S6	Invalidate configuration	Off = Normal On = Clears NVRAM
S7	Reserved	Reserved
S8	Reserved	Reserved

To change the system configuration at a later time, refer to the procedure above to set back the S2 switch to **Off**, modify the configuration as necessary then set back the S2 switch to **On**.

NOTE

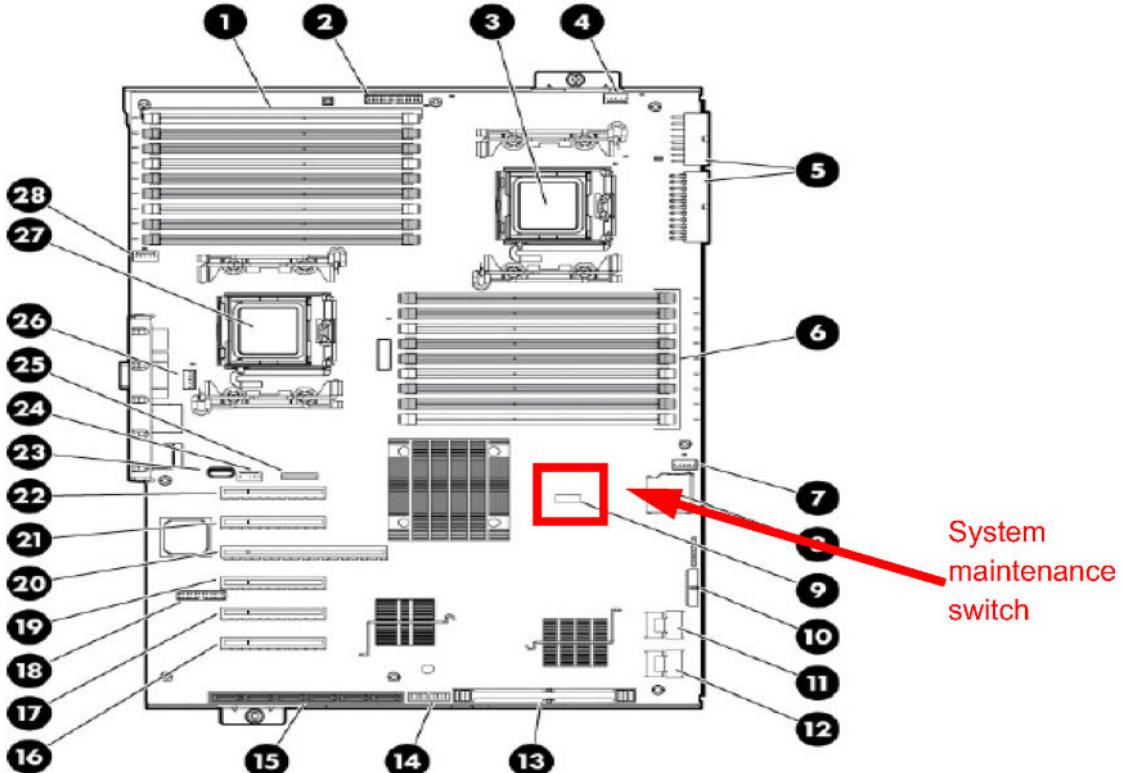
S1 switch: In case the ILO password would be lost or corrupted, you should power off the system, set the S1 switch to **On**, power on the system again, login to the ILO, set a new password, then power off the server and set the S1 switch back to **Off** to enable ILO security

A.22.1.6 HPE ProLiant ML350p Gen8 Server hardware security setup

Pre-requisite: The software is loaded on the server.

1. Shutdown the server, following the proper shutdown procedures (I.e: sending first a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cables if their length is insufficient to allow moving out the server.
3. Remove the front bezel before tilting the server on the side.
4. Open the access panel.

5. Locate the System maintenance switch.



6. Setup the System maintenance switch.

System maintenance switch

The system maintenance switch (SW1) is a ten-position switch that is used for system configuration. The default position for all positions is **Off**.

- To lockup system configuration, once configuration has been setup to your needs, move the **S2** switch of the System maintenance switch to **On**. Then reconnect the power supplies to the mains and reboot the server.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.
S3	Reserved	Reserved
S4	Reserved	Reserved
S5	Password protection override	Off = No function On = Clears power-on and administrator password(s)
S6	Invalidate configuration	Off = Normal On = Clears NVRAM
S7 - S10	Reserved	Reserved

To change the system configuration at a later time, refer to the procedure above to set back the S2 switch to **Off**, modify the configuration as necessary then set back the S2 switch to **On**.

NOTE

S1 switch: In case the ILO password would be lost or corrupted, you should power off the system, set the S1 switch to **On**, power on the system again, login to the ILO, set a

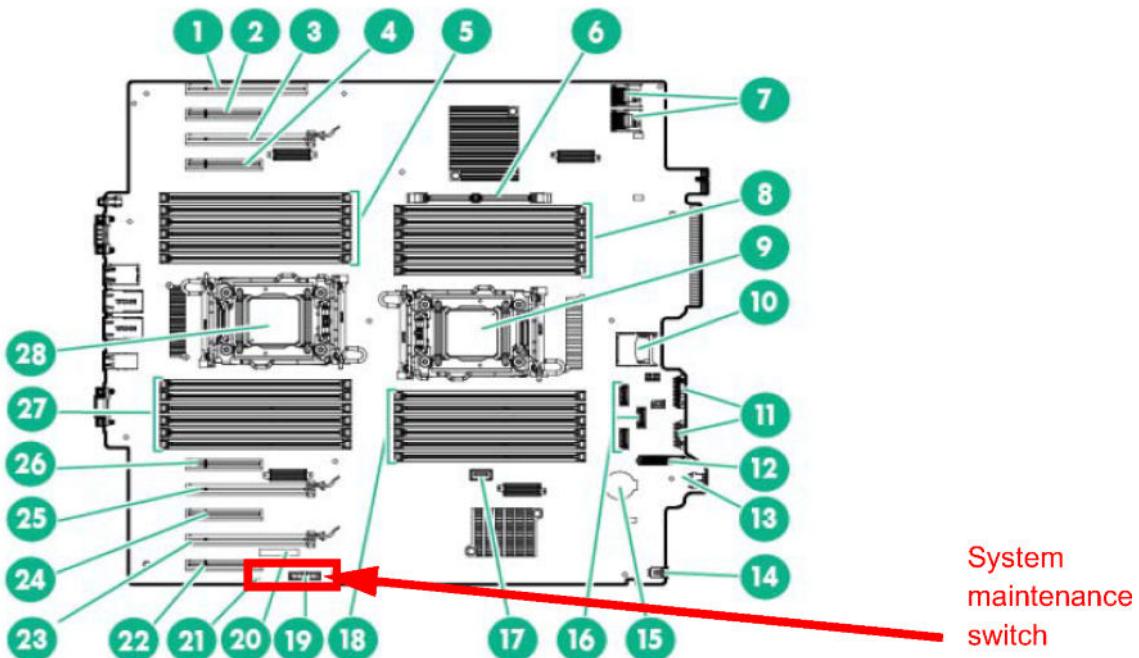
new password, then power off the server and set the S1 switch back to **Off** to enable ILO security.

A.22.1.7 HP ProLiant ML350 G6 Server hardware security setup

NOTE

You may need to request access to the servers room from the IT administrator of the site, in case of rackable units.

1. Shutdown the server, following the proper shutdown procedures (i.e: sending first a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cables if there length is insufficient to allow moving out the server.
3. Remove the front bezel before tilting the server on the side.
4. Open the access panel
5. Locate the System maintenance switch.
6. Setup the System maintenance switch.



System maintenance switch

The system maintenance switch (SW1) is a twelve-position switch that is used for system configuration. The default position for all positions is **Off**.

- To lockup system configuration, once configuration has been setup to your needs, move the **S2** switch of the System maintenance switch to **On**. Then reconnect the power supplies to the mains and reboot the server.

Position	Description	Function
S1	iLO security	Off = iLO security is enabled. On = iLO security is disabled.
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.

Position	Description	Function
S3	Reserved	Off = Tower On = rack (to be set when using the rack option)
S4	Reserved	Reserved
S5	Password protection override	Off = No function On = Clears power-on and administrator password(s)
S6	Invalidate configuration	Off = Normal On = ROM treats the system configuration as invalid
S7 - S12	Reserved	Reserved

To change the system configuration at a later time, refer to the procedure above to set back the S2 switch to **Off**, modify the configuration as necessary then set back the S2 switch to **On**.

NOTE

S1 switch: In case the ILO password would be lost or corrupted, you should power off the system, set the S1 switch to **On**, power on the system again, login to the ILO, set a new password, then power off the server and set the S1 switch back to **Off** to enable ILO security

A.22.2 Removing passwords or recovering from password loss

The following intends to give you guidelines in order to remove any password entered for your hardware, or clear the lock for the server hardware BIOS, in case of loss of the BIOS administration password previously setup for your hardware.

NOTE

You may need to request access to the servers room from the IT administrator of the site, in case of rackable units to be unlocked.

1. Shutdown the server, following the proper shutdown procedures (I.e: sending first a broadcast message if the server is in use). Refer to the AW Server 3.2 Installation and Service Manual for instructions.
2. Once the server has turned off, disconnect all power supplies from the power line. Also disconnect any cables if their length is insufficient to allow moving out the server.
3. Open the access panel of the server.

NOTICE

The boards and disk drives contain electronic **components that are extremely sensitive to static electricity**. Do not touch the components themselves or any metal parts. Carefully observe electrostatic discharge precautions when servicing inside the unit. Use a grounding wrist wrap and/or anti-static mat when handling the drive assemblies, boards or cards.

4. Locate the System maintenance switch.
5. Setup the System maintenance switch in order to remove the lock (move the **S2** switch of the System maintenance switch to **OFF**).

Position	Description	Function
S2	Configuration lock	Off = System configuration can be changed. On = System configuration is locked.

6. Reconnect the power supplies to the mains and reboot the server. You are now able to make any necessary modification to the BIOS and/or the boot sequence.
7. Remove passwords from hardware level:

To recover the server from a password that is lost or forgotten, below are the steps to reset the server from system board level.

- Turn OFF the server and remove the top/side cover so that user can see the system board.
- Locate the System Maintenance Switch on the system board, refer to the server documentation or the diagram on the hood label.
- Remove any air baffle or fans or add-on cards which are blocking the access to system maintenance switch.

To reset the Power-On Password:

- Set switch#5 to ON position and turn ON the server. Once the password is cleared, turn OFF the server and put the switch#5 to its default position. Turn ON the server and now user may set a new Power-On Password if required.

To reset the Admin Password:

- Set switch#6 to ON position and remove the CMOS Battery. Wait for a minute and put the battery back into its position and turn ON the server. The settings will be restored, now switch OFF the server and put the switch#6 to its default position. Turn ON the server and now user may set a new Admin Password if required.

NOTE

When the system maintenance switch position 6 is set to the ON position, the system is prepared to erase all system configuration settings from both CMOS and NVRAM.

NOTICE

Careful: Clearing CMOS and/or NVRAM deletes all BIOS configuration information. Be sure to properly re-configure the server BIOS prior to use the server. Failing to do so, data loss could occur.

8. When done, it is strongly recommended that you set back hardware protection, by entering a new password for the BIOS administration, (see the AW Server 3.2 Hardware Installation Manual, Setting up a BIOS administrator password) then proceeding to configuration lock, by setting back the S2 switch to ON.

A.23 RPM2CPIO

rpm2cpio is a Linux command which allows, in combination with **cpio** command (another Linux command), to extract files from an RPM package.

This tool is very useful to extract files from RPM packages at anytime, especially when there is a need to restore files that have been corrupted by the system without needing to install the packages.

And so to avoid a full re-installation of the system.

- **rpm2cpio** is not a GEHC service tool (as well as **cpio**)
- **rpm2cpio** is already part of the Linux OS tool-set. (as well as **cpio**)

USE CASE - Extract file/directory from the AW Server Platform media and restore it into the correct AWS location

RPM Package	File/Directory Path in RPM	File/Directory Location in AWS
RPM_Package	File_Directory_Path_in_RPM	File_Directory_Location_in_AWS

In the following steps, replace RPM_Package, File_Directory_Path_in_RPM and File_Directory_Location_in_AWS by the correct value.

- The following steps shall be performed only once, even if several files/directories needs to be restored:

- Insert the AW Server Platform media.
- Open a Terminal from **Service Tools > Tools** and login as **root**.
- At the command prompt, create a mount point for the platform media:

```
mkdir /mnt/media <Enter>
```

- Mount the platform software media:

```
mount /dev/sr0 /mnt/media <Enter>
```

- Change to the root directory:

```
cd / <Enter>
```

- Locate the RPM package, containing the file(s) you want to extract, from the media:

```
find /mnt/media -name "*.rpm" -print | grep -i RPM_Package <Enter>
```

The path of the package displays (note it):

RPM_Path

- Cleanup tmp/extract_rpm directory used to extract the package:

```
rm -rf /tmp/extract_rpm
```

```
mkdir /tmp/extract_rpm
```

```
cd /tmp/extract_rpm <Enter>
```

- Extract the files from the RPM package and copy them into /tmp location:

```
rpm2cpio RPM_Path | cpio -uidmv <Enter>
```

- Copy the file (or directory) to the right location:

- To copy a file, type: /bin/cp File_Directory_Path_in_RPM File_Directory_Location_in_AWS

- To copy a directory, type: /bin/cp -rf File_Directory_Path_in_RPM File_Directory_Location_in_AWS

- Unmount the media:

```
umount /dev/sr0 <Enter>
```

- Eject the media if not needed anymore:

```
eject cdrom <Enter>
```

A.24 AW Server enhanced security configuration

This section describes how to configure the AW Server for enhanced security.

The Advanced Service Manual Addendum (5831227-1EN Rev 1 or higher) addendum has been created for that purpose. It describes the procedure to configure the AW Server 3.2 systems to meet US Department of Defense (DoD) requirements.

This Installation Manual addendum is to be used after installing the AW Server 3.2 Ext.3.2 release (or higher) on a DoD site in the United States.



www.gehealthcare.com