



## AW Server 3.2 Ext. 4.9

### Installation Manual

#### AW Server 3.2 Ext. 4.9

##### **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 and 11.

Certain GE consoles are also supported. See the corresponding console User Guides for further details.

Browsers: Firefox®, Chrome®, Microsoft Edge®, Safari®

##### **Client for Windows**

Version 3.2 Ext. 4.9

[Download](#)

##### **AW**

[Launch](#)

##### **Service and Administrative Tools**

[Launch](#)

##### **AW Server / Application User Manuals**

[Open](#)

##### **Regulatory Information**

[Open](#)

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

Windows and Microsoft Edge 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.

5922979-8EN  
Revision 2

*General service documentation.*

© 2023 GE HealthCare. GE is a trademark of General Electric Company used under trademark license.  
Reproduction and/or distribution is prohibited.

# Language Policy

## DOC0371395 - Global Language Procedure

ПРЕДУПРЕЖДЕНИЕ (BG)	<p>Това упътване за работа е налично само на английски език.</p> <ul style="list-style-type: none"> <li>Ако доставчикът на услугата на клиента изиска друг език, задължение на клиента е да осигури превод.</li> <li>Не използвайте оборудването, преди да сте се консултирали и разбрали упътването за работа.</li> <li>Неспазването на това предупреждение може да доведе до нараняване на доставчика на услугата, оператора или пациента в резултат на токов удар, механична или друга опасност.</li> </ul>
警告 (ZH-CN)	<p>本维修手册仅提供英文版本。</p> <ul style="list-style-type: none"> <li>如果客户的维修服务人员需要非英文版本，则客户需自行提供翻译服务。</li> <li>未详细阅读和完全理解本维修手册之前，不得进行维修。</li> <li>忽略本警告可能对维修服务人员、操作人员或患者造成电击、机械伤害或其他形式的伤害。</li> </ul>
警告 (ZH-HK)	<p>本服務手冊僅提供英文版本。</p> <ul style="list-style-type: none"> <li>倘若客戶的服務供應商需要英文以外之服務手冊，客戶有責任提供翻譯服務。</li> <li>除非已參閱本服務手冊及明白其內容，否則切勿嘗試維修設備。</li> <li>不遵從本警告或會令服務供應商、網絡供應商或病人受到觸電、機械性或其他的危險。</li> </ul>
警告 (ZH-TW)	<p>本维修手册仅有英文版。</p> <ul style="list-style-type: none"> <li>若客戶的維修廠商需要英文版以外的語言，應由客戶自行提供翻譯服務。</li> <li>請勿試圖維修本設備，除非您已查閱並瞭解本維修手冊。</li> <li>若未留意本警告，可能導致維修廠商、操作員或病患因觸電、機械或其他危險而受傷。</li> </ul>
UPOZORENJE (HR)	<p>Ovaj servisni priručnik dostupan je na engleskom jeziku.</p> <ul style="list-style-type: none"> <li>Ako davatelj usluge klijenta treba neki drugi jezik, klijent je dužan osigurati prijevod.</li> <li>Ne pokušavajte servisirati opremu ako niste u potpunosti pročitali i razumjeli ovaj servisni priručnik.</li> <li>Zanemarite li ovo upozorenje, može doći do ozljede davatelja usluge, operatera ili pacijenta uslijed strujnog udara, mehaničkih ili drugih rizika.</li> </ul>
VÝSTRAHA (CS)	<p>Tento provozní návod existuje pouze v anglickém jazyce.</p> <ul style="list-style-type: none"> <li>V případě, že externí služba zákazníkům potřebuje návod v jiném jazyce, je zajištění překladu do odpovídajícího jazyka úkolem zákazníka.</li> <li>Nesnažte se o údržbu tohoto zařízení, aniž byste si přečetli tento provozní návod a pochopili jeho obsah.</li> <li>V případě nedodržování této výstrahy může dojít k poranění pracovníka prodejního servisu, obslužného personálu nebo pacientů vlivem elektrického proudu, respektive vlivem mechanických či jiných rizik.</li> </ul>
ADVARSEL (DA)	<p>Denne servicemanual findes kun på engelsk.</p> <ul style="list-style-type: none"> <li>Hvis en kundes tekniker har brug for et andet sprog end engelsk, er det kundens ansvar at sørge for oversættelse.</li> <li>Forsøg ikke at servicere udstyret uden at læse og forstå denne servicemanual.</li> <li>Manglende overholdelse af denne advarsel kan medføre skade på grund af elektrisk stød, mekanisk eller anden fare for teknikeren, operatøren eller patienten.</li> </ul>

WAARSCHUWING (NL)	<p>Deze onderhoudshandleiding is enkel in het Engels verkrijgbaar.</p> <ul style="list-style-type: none"> <li>Als het onderhoudspersoneel een andere taal vereist, dan is de klant verantwoordelijk voor de vertaling ervan.</li> <li>Probeer de apparatuur niet te onderhouden alvorens deze onderhoudshandleiding werd geraadpleegd en begrepen is.</li> <li>Indien deze waarschuwing niet wordt opgevolgd, zou het onderhoudspersoneel, de operator of een patiënt gewond kunnen raken als gevolg van een elektrische schok, mechanische of andere gevaren.</li> </ul>
WARNING (EN)	<p>This service manual is available in English only.</p> <ul style="list-style-type: none"> <li>If a customer's service provider requires a language other than English, it is the customer's responsibility to provide translation services.</li> <li>Do not attempt to service the equipment unless this service manual has been consulted and is understood.</li> <li>Failure to heed this warning may result in injury to the service provider, operator or patient from electric shock, mechanical or other hazards.</li> </ul>
HOIATUS (ET)	<p>See teenindusjuhend on saadaval ainult inglise keeles.</p> <ul style="list-style-type: none"> <li>Kui klienditeeninduse osutaja nõuab juhendit inglise keest erinevas keeles, vastutab klient tõlketeenuse osutamise eest.</li> <li>Ärge üritage seadmeid teenindada enne eelnevalt käesoleva teenindusjuhendiga tutvumist ja sellest aru saamist.</li> <li>Käesoleva hoiatuse eiramise võib põhjustada teenuseosutaja, operaatori või patsiendi vigastamist elektrilöögi, mehaanilise või muu ohu tagajärvel.</li> </ul>
VAROITUS (FI)	<p>Tämä huolto-ohje on saatavilla vain englanniksi.</p> <ul style="list-style-type: none"> <li>Jos asiakkaan huoltohenkilöstö vaatii muuta kuin englanninkielistä materiaalia, tarvittavan käänöksen hankkiminen on asiakkaan vastuulla.</li> <li>Älä yritykseen korjata laitteista ennen kuin olet varmasti lukenut ja ymmärtänyt tämän huolto-ohjeen.</li> <li>Mikäli tästä varoitusta ei noudata, seuraaksena voi olla huoltohenkilöstön, laitteiston käyttäjän tai potilaan vahingoittuminen sähköiskun, mekaanisen vian tai muun vaaratilanteen vuoksi.</li> </ul>
ATTENTION (FR)	<p>Ce manuel d'installation et de maintenance est disponible uniquement en anglais.</p> <ul style="list-style-type: none"> <li>Si le technicien d'un client a besoin de ce manuel dans une langue autre que l'anglais, il incombe au client de le faire traduire.</li> <li>Ne pas tenter d'intervenir sur les équipements tant que ce manuel d'installation et de maintenance n'a pas été consulté et compris.</li> <li>Le non-respect de cet avertissement peut entraîner chez le technicien, l'opérateur ou le patient des blessures dues à des dangers électriques, mécaniques ou autres.</li> </ul>
WARNUNG (DE)	<p>Diese Serviceanleitung existiert nur in englischer Sprache.</p> <ul style="list-style-type: none"> <li>Falls ein fremder Kundendienst eine andere Sprache benötigt, ist es Aufgabe des Kunden für eine entsprechende Übersetzung zu sorgen.</li> <li>Versuchen Sie nicht diese Anlage zu warten, ohne diese Serviceanleitung gelesen und verstanden zu haben.</li> <li>Wird diese Warnung nicht beachtet, so kann es zu Verletzungen des Kundendiensttechnikers, des Bedieners oder des Patienten durch Stromschläge, mechanische oder sonstige Gefahren kommen.</li> </ul>
ΠΡΟΕΙΔΟΠΟΙΗΣΗ (EL)	<p>Τοπαρόν εγχειρίδιο σέρβις διατίθεται στα αγγλικά μόνο.</p> <ul style="list-style-type: none"> <li>Εάν το άτομο παροχής σέρβις ενός πελάτη απαιτεί το παρόν εγχειρίδιο σε γλώσσα εκτός των αγγλικών, αποτελεί ευθύνη του πελάτη να παρέχει υπηρεσίες μετάφρασης.</li> <li>Μηνεπιχειρήσετε την εκτέλεση εργασιών σέρβις στον εξοπλισμό εκτός εάν έχετε συμβουλευτεί και έχετε κατανοήσει το παρόν εγχειρίδιο σέρβις.</li> <li>Εάν δεν λάβετε υπόψη την προειδοποίηση αυτή, ενδέχεται να προκληθεί τραυματισμός στο άτομο παροχής σέρβις, στο χειριστή ή στον ασθενή από ηλεκτροπληξία, μηχανικούς ή άλλους κινδύνους.</li> </ul>

FIGYELMEZ-TETÉS (HU)	Ezen karbantartási kézikönyv kizárólag angol nyelven érhető el. <ul style="list-style-type: none"> <li>Ha a vevő szolgáltatója angoltól eltérő nyelvre tart igényt, akkor a vevő felelőssége a fordítás elkészítése.</li> <li>Ne próbálja elkezdeni használni a berendezést, amíg a karbantartási kézikönyvben leírtakat nem értelmezték.</li> <li>Ezen figyelmeztetés figyelmen kívül hagyása a szolgáltató, működtető vagy a beteg áramütés, mechanikai vagy egyéb veszélyhelyzet miatti sérülését eredményezheti.</li> </ul>
AÐVÖRUN (IS)	Þessi þjónustuhandbók er aðeins fáanleg á ensku. <ul style="list-style-type: none"> <li>Ef að þjónustuveitandi viðskiptamanns þarfnað annas tungumáls en ensku, er það skylda viðskiptamanns að skaffa tungumálaþjónustu.</li> <li>Reynið ekki að afgreiða tækið nema að þessi þjónustuhandbók hefur verið skoðuð og skilin.</li> <li>Brot á sinna þessari aðvörun getur leitt til meiðsla á þjónustuveitanda, stjórnanda eða sjúklings frá raflosti, vélraenu eða öðrum áhættum.</li> </ul>
AVVERTENZA (IT)	Il presente manuale di manutenzione è disponibile soltanto in lingua inglese. <ul style="list-style-type: none"> <li>Se un addetto alla manutenzione richiede il manuale in una lingua diversa, il cliente è tenuto a provvedere direttamente alla traduzione.</li> <li>Procedere alla manutenzione dell'apparecchiatura solo dopo aver consultato il presente manuale ed averne compreso il contenuto.</li> <li>Il mancato rispetto della presente avvertenza potrebbe causare lesioni all'addetto alla manutenzione, all'operatore o ai pazienti provocate da scosse elettriche, urti meccanici o altri rischi.</li> </ul>
警告 (JA)	このサービスマニュアルには英語版しかありません。 <ul style="list-style-type: none"> <li>サービスを担当される業者が英語以外の言語を要求される場合、翻訳作業はその業者の責任で行うものとさせていただきます。</li> <li>このサービスマニュアルを熟読し理解せずに、装置のサービスを行わないでください。</li> <li>この警告に従わない場合、サービスを担当される方、操作員あるいは患者さんが、感電や機械的又はその他の危険により負傷する可能性があります。</li> </ul>
경고 (KO)	본 서비스 매뉴얼은 영어로만 이용하실 수 있습니다. <ul style="list-style-type: none"> <li>고객의 서비스 제공자가 영어 이외의 언어를 요구할 경우, 번역 서비스를 제공하는 것은 고객의 책임입니다.</li> <li>본 서비스 매뉴얼을 참조하여 숙지하지 않은 이상 해당 장비를 수리하려고 시도하지 마십시오.</li> <li>본 경고 사항에 유의하지 않으면 전기 쇼크, 기계적 위험, 또는 기타 위험으로 인해 서비스 제공자, 사용자 또는 환자에게 부상을 입힐 수 있습니다.</li> </ul>
BRĪDINĀ-JUMS (LV)	Šī apkopes rokasgrāmata ir pieejama tikai anglu valodā. <ul style="list-style-type: none"> <li>Ja klienta apkopes sniedzējam nepieciešama informācija citā valodā, klienta pienākums ir nodrošināt tulkojumu.</li> <li>Neveiciet aprīkojuma apkopi bez apkopes rokasgrāmatas izlasīšanas un saprašanas.</li> <li>Šī brīdinājuma neievērošanas rezultātā var rasties elektriskās strāvas trieciena, mehānisku vai citu faktoru izraisītu traumu risks apkopes sniedzējam, operatoram vai pacientam.</li> </ul>
ISPĒJIMAS (LT)	Šis ekspluatavimo vadovas yra tik anglų kalba. <ul style="list-style-type: none"> <li>Jei kliento paslaugų tiekėjas reikalauja vadovo kita kalba – ne anglų, suteikti vertimo paslaugas privalo klientas.</li> <li>Neméginkite atlirkiti įrangos techninės priežiūros, jei neperskaitėte ar nesupratote šio ekspluatavimo vadovo.</li> <li>Jei nepaisysite šio įspėjimo, galimi paslaugų tiekėjo, operatoriaus ar paciento sužalojimai dėl elektros šoko, mechaninių ar kitų pavojų.</li> </ul>

ADVARSEL (NO)	<p>Denne servicehåndboken finnes bare på engelsk.</p> <ul style="list-style-type: none"> <li>Hvis kundens serviceleverandør har bruk for et annet språk, er det kundens ansvar å sørge for oversettelse.</li> <li>Ikke forsøk å reparere utstyret uten at denne servicehåndboken er lest og forstått.</li> <li>Manglende hensyn til denne advarselen kan føre til at serviceleverandøren, operatøren eller pasienten skades på grunn av elektrisk støt, mekaniske eller andre farer.</li> </ul>
OSTRZEŻE- NIE (PL)	<p>Niniejszy podręcznik serwisowy dostępny jest jedynie w języku angielskim.</p> <ul style="list-style-type: none"> <li>Jeśli serwisant klienta wymaga języka innego niż angielski, zapewnienie usługi tłumaczenia jest obowiązkiem klienta.</li> <li>Nie próbować serwisować urządzenia bez zapoznania się z niniejszym podręcznikiem serwisowym i zrozumienia go.</li> <li>Niezastosowanie się do tego ostrzeżenia może doprowadzić do obrażeń serwisanta, operatora lub pacjenta w wyniku porażenia prądem elektrycznym, zagrożenia mechanicznego bądź innego.</li> </ul>
ATENÇÃO (PT-BR)	<p>Este manual de assistência técnica encontra-se disponível unicamente em inglês.</p> <ul style="list-style-type: none"> <li>Se outro serviço de assistência técnica solicitar a tradução deste manual, caberá ao cliente fornecer os serviços de tradução.</li> <li>Não tente reparar o equipamento sem ter consultado e compreendido este manual de assistência técnica.</li> <li>A não observância deste aviso pode ocasionar ferimentos no técnico, operador ou paciente decorrentes de choques elétricos, mecânicos ou outros.</li> </ul>
ATENÇÃO (PT-PT)	<p>Este manual de assistência técnica só se encontra disponível em inglês.</p> <ul style="list-style-type: none"> <li>Se qualquer outro serviço de assistência técnica solicitar este manual noutro idioma, é da responsabilidade do cliente fornecer os serviços de tradução.</li> <li>Não tente reparar o equipamento sem ter consultado e compreendido este manual de assistência técnica.</li> <li>O não cumprimento deste aviso pode colocar em perigo a segurança do técnico, do operador ou do paciente devido a choques eléctricos, mecânicos ou outros.</li> </ul>
ATENȚIE (RO)	<p>Acest manual de service este disponibil doar în limba engleză.</p> <ul style="list-style-type: none"> <li>Dacă un furnizor de servicii pentru clienți necesită o altă limbă decât cea engleză, este de datoria clientului să furnizeze o traducere.</li> <li>Nu încercați să reparați echipamentul decât ulterior consultării și înțelegerea acestui manual de service.</li> <li>Ignorarea acestui avertisment ar putea duce la rănirea depanatorului, operatorului sau pacientului în urma pericolelor de electrocutare, mecanice sau de altă natură.</li> </ul>
ОСТОРОЖНО ! (RU)	<p>Данное руководство по техническому обслуживанию представлено только на английском языке.</p> <ul style="list-style-type: none"> <li>Если сервисному персоналу клиента необходимо руководство не на английском, а на каком-то другом языке, клиенту следует самостоятельно обеспечить перевод.</li> <li>Перед техническим обслуживанием оборудования обязательно обратитесь к данному руководству и поймите изложенные в нем сведения.</li> <li>Несоблюдение требований данного предупреждения может привести к тому, что специалист по техобслуживанию, оператор или пациент получит удар электрическим током, механическую травму или другое повреждение.</li> </ul>
UPOZORENJE (SR)	<p>Ovo servisno uputstvo je dostupno samo na engleskom jeziku.</p> <ul style="list-style-type: none"> <li>Ako klijentov serviser zahteva neki drugi jezik, klijent je dužan da obezbedi prevodilačke usluge.</li> <li>Ne pokušavajte da opravite uređaj ako niste pročitali i razumeli ovo servisno uputstvo.</li> <li>Zanemarivanje ovog upozorenja može dovesti do povredovanja servisera, rukovaoca ili pacijenta usled strujnog udara ili mehaničkih i drugih opasnosti.</li> </ul>

UPOZORNE-NIE (SK)	Tento návod na obsluhu je k dispozícii len v angličtine. <ul style="list-style-type: none"> <li>• Ak zákazníkov poskytovateľ služieb vyžaduje iný jazyk ako angličtinu, poskytnutie prekladateľských služieb je zodpovednosťou zákazníka.</li> <li>• Nepokúšajte sa o obsluhu zariadenia, kým si neprečítate návod na obchu a nepoznamiete mu.</li> <li>• Zanedbanie tohto upozornenia môže spôsobiť zranenie poskytovateľa služieb, obsluhujúcej osoby alebo pacienta elektrickým prúdom, mechanické alebo iné ohrozenie.</li> </ul>
ATENCIÓN (ES)	Este manual de servicio sólo existe en inglés. <ul style="list-style-type: none"> <li>• Si el encargado de mantenimiento de un cliente necesita un idioma que no sea el inglés, el cliente deberá encargarse de la traducción del manual.</li> <li>• No se deberá dar servicio técnico al equipo, sin haber consultado y comprendido este manual de servicio.</li> <li>• La no observancia del presente aviso puede dar lugar a que el proveedor de servicios, el operador o el paciente sufran lesiones provocadas por causas eléctricas, mecánicas o de otra naturaleza.</li> </ul>
VARNING (SV)	Den här servicehandboken finns bara tillgänglig på engelska. <ul style="list-style-type: none"> <li>• Om en kunds servicetekniker har behov av ett annat språk än engelska, ansvarar kunden för att tillhandahålla översättningstjänster.</li> <li>• Försök inte utföra service på utrustningen om du inte har läst och förstått den här servicehandboken.</li> <li>• Om du inte tar hänsyn till den här varningen kan det resultera i skador på serviceteknikern, operatören eller patienten till följd av elektriska stötar, mekaniska faror eller andra faror.</li> </ul>
OPOZORILO (SL)	Ta servisni priročnik je na voljo samo v angleškem jeziku. <ul style="list-style-type: none"> <li>• Če ponudnik storitve stranke potrebuje priročnik v drugem jeziku, mora stranka zagotoviti prevod.</li> <li>• Ne poskušajte servisirati opreme, če tega priročnika niste v celoti prebrali in razumeli.</li> <li>• Če tega opozorila ne upoštevate, se lahko zaradi električnega udara, mehanskih ali drugih nevarnosti poškoduje ponudnik storitev, operater ali bolnik.</li> </ul>
DİKKAT (TR)	Bu servis kılavuzunun sadece ingilizcesi mevcuttur. <ul style="list-style-type: none"> <li>• Eğer müşteri teknisyeni bu kılavuzu ingilizce dışında bir başka lisandan talep ederse, bunu tercüme ettmek müşteriye düşer.</li> <li>• Servis kılavuzunu okuyup anlamadan ekipmanlara müdahale etmeyiniz.</li> <li>• Bu uyarıyla uyulmaması, elektrik, mekanik veya diğer tehlikelerden dolayı teknisyen, operatör veya hastanın yaralanmasına yol açabilir.</li> </ul>
ЗАСТЕРЕЖЕНИЯ (UK)	Даний посібник з експлуатації доступний тільки англійською мовою. <ul style="list-style-type: none"> <li>• Якщо постачальник послуг клієнта спілкується іноземною мовою, тоді клієнт зобов'язаний забезпечити переклад.</li> <li>• Заборонено проводити огляд обладнання без попереднього звертання до даного посібника з експлуатації і розуміння інформації, поданої у ньому.</li> <li>• Недотримання цього застереження може завдати шкоди здоров'ю постачальника послуг, оператора або пацієнта через ураження електричним струмом, механічну травму або інше ушкодження.</li> </ul>

## Legal Notes

## Trademarks

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

## 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

## Omissions & Errors

Customers, please contact your GE Sales or Service representatives.

GE personnel, please use the GEHC TrackWise Process to report all omissions, errors, and defects in this publication.

## Electrical Contractors

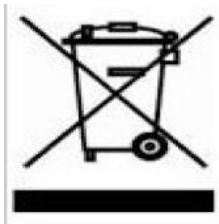
### Certified Electrical Contractor Statement

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 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 **DOC2781870**.

Release of this document is referenced and archived in TechPub as **5922979-8EN**.

The reference of the previous version of this document is 5884093-8EN.

Revision	Date	Reason for change
1	February 3 <sup>rd</sup> , 2023	Initial release for AW Server 3.2 Ext. 4.9: SPR HCSDM00694468 SPR HCSDM00717108
2	July 13, 2023	Second release for the update of the NanoCloud AW Server Installation procedures: SPR HCSDM00724730 / SPR HCSDM00739976 / SPR HCSDM00742184

# Contents

<b>Chapter 1 Getting Started.....</b>	<b>20</b>
1.1 Publication conventions .....	20
1.1.1 Intent of Information .....	20
1.1.2 Safety Terminology .....	20
1.1.3 Data Entry Formatting Conventions .....	21
1.1.4 Information Disclaimer .....	21
1.1.5 Contents of this document.....	21
1.2 Access to Documentation and Service links .....	22
1.2.1 Documentation .....	22
1.2.1.1 Access the AW Server 3.2 Service Documentation .....	22
1.2.1.2 Navigating back and forth though cross-reference links in PDF files.....	22
1.2.2 Service Web links .....	23
1.3 Software Kit .....	23
1.3.1 Physical Software Kit .....	23
1.3.2 Digital Software Kit .....	25
1.4 Identification of Software releases.....	27
1.5 LOTO Warning.....	27
1.6 Supported Web Browsers .....	27
<b>Chapter 2 Installation of a new AW Server.....</b>	<b>29</b>
2.1 Overview.....	29
2.2 AW Server - Product Description .....	29
2.2.1 GEHC delivered AW Server hardware.....	29
2.2.1.1 The low-tier rack-mount version.....	29
2.2.1.2 The high-tier rack-mount version .....	29
2.2.2 Hypervisor environments for Virtual AW Server.....	30
2.2.3 The AW Server – system components .....	30
2.2.4 Software Changes .....	30
2.2.5 Before you start.....	30
2.2.6 Software preload by Manufacturing.....	31
2.2.6.1 GEHC delivered Physical servers.....	31
2.2.6.2 Virtual AW Servers on customer's physical servers.....	31
2.3 Quick Start Installation Guide - Physical AW Server .....	31
2.3.1 Physical AW Server Characteristics .....	32
2.3.2 Physical AW Server Installation steps overview .....	32
2.4 Quick Start Installation Guide - Virtual AW Server .....	35
2.4.1 Virtual AW Server Characteristics .....	36
2.4.2 Virtual AW Server Installation steps overview .....	38
2.4.3 Quick Start Installation Guide - Scalable Virtual servers.....	42
2.5 Job Card IST001A - Hardware Installation Verification.....	45
2.5.1 Time Reporting for Installation and Warranty .....	45
2.5.2 Hardware Installation validation.....	46
2.5.3 HPE ProLiant DL360 Gen10 Server High Tier and Low Tier.....	46
2.5.4 Finalizing Installation Verification.....	50
2.5.5 iLO Service Processor Firmware upgrade .....	55

---

2.6 Job Card IST001AB - Hypervisor Configuration .....	59
2.6.1 Overview.....	59
2.6.2 Ethernet ports Allocation.....	60
2.6.2.1 Foreword .....	60
2.6.2.2 Procedure .....	61
2.6.3 Create a GEHC service user account.....	63
2.6.4 Setup a NTP server for the Hypervisor .....	67
2.7 Job Card IST001B - Virtual Machine creation .....	68
2.7.1 Overview.....	68
2.7.2 Virtual machine creation .....	70
2.7.2.1 OVF Template Installation .....	71
2.7.2.2 Steps to upgrade / downgrade a Virtual Machine .....	75
2.7.2.3 Creating the image data disk for Standalone (Non-Integrated) and Hybrid AW Server ...	77
2.8 Job Card IST001C - Virtual Servers Cluster Installation Steps.....	80
2.8.1 Foreword .....	80
2.8.1.1 Pre-requisites for Cluster operation.....	80
2.8.2 Preliminary Steps.....	81
2.8.2.1 Virtual machine resources for AW Server .....	81
2.8.2.2 Physical Network configuration .....	81
2.8.3 Installation and configuration Steps .....	83
2.8.3.1 Hypervisor pre-requisites .....	83
2.8.3.2 Ethernet ports allocation.....	84
2.8.3.3 GE Service account setup .....	84
2.8.3.4 NTP server setup for the Virtual AW Servers / HAPS servers .....	84
2.8.3.5 Virtual Machine (VM) creation .....	84
2.8.3.6 AW Server / HAPS server installation and configuration.....	84
2.8.4 Scalability Installation Checklist .....	84
2.8.4.1 Under Site IT administrator responsibility .....	84
2.8.4.2 Under GEHC FE responsibility .....	85
2.9 Job Card IST002B - Virtual Machine Installation Verification .....	87
2.9.1 Retrieving the MAC address.....	88
2.9.2 Verifying the Virtual Machine.....	89
2.10 Job Card IST002C - Installation Wizard - Prepare and perform the AW Server configuration .....	90
2.10.1 Overview.....	90
2.10.2 Preparing the AW Server configuration.....	90
2.10.2.1 Launching the Installation Wizard .....	90
2.10.2.2 Starting the Installation Wizard configuration .....	91
2.10.2.3 Installation Wizard navigation and Field Filling Rules .....	93
2.10.2.4 Configuring the network and time settings.....	94
2.10.2.5 Configuring the licensing settings.....	95
2.10.2.6 Configuring the platform settings.....	96
2.10.2.7 Configuring the license server(s) settings .....	96
2.10.2.8 Configuring DICOM hosts.....	98
2.10.2.9 Filling out the device information.....	100
2.10.2.10 Configuring End of Review .....	101
2.10.2.11 Saving the configuration .....	102
2.10.3 Perform the AW Server configuration .....	103
2.10.4 Reenable the Cloud-init mechanism.....	106
2.11 Job Card IST003 - Installation of Platform Software .....	109
2.11.1 AWS Platform software load preparation .....	109

2.11.1.1 Physical AW servers .....	109
2.11.1.2 Virtual AW Server .....	109
2.11.2 AWS platform software load .....	113
2.11.3 HAPS Server installation.....	122
2.12 Job Card IST004A - HPE R/T3000 UPS drivers setup.....	123
2.12.1 HPE R/T3000 UPS drivers installation verification .....	124
2.12.2 Configuring the HPE R/T3000 UPS using HPPP Software .....	124
2.13 Job Card IST005 - Network and Time Configuration.....	127
2.13.1 Network Configuration .....	128
2.13.1.1 Important information about Hostname.....	128
2.13.1.2 Network Configuration Procedure .....	128
2.13.2 Date and Time Configuration .....	129
2.13.3 Reboot the AW Server .....	131
2.14 Job Card IST007 - Service Tools Login.....	131
2.14.1 Logging into Service Tools.....	131
2.14.2 HealthPage Examples .....	134
2.14.2.1 HealthPage Status example- HP server .....	134
2.14.2.2 HealthPage "Status" example- Virtual server.....	134
2.14.2.3 HealthPage "System Configuration" example.....	135
2.14.2.4 HealthPage "Remote Service" example.....	135
2.14.2.5 HealthPage "Version Information" example .....	136
2.14.2.6 HealthPage "Configuration & Status" display .....	136
2.14.2.7 HealthPage "Software Subsystem" example.....	137
2.14.3 Navigating in Service Tools.....	138
2.15 Job Card IST008 - Initial Configuration .....	140
2.15.1 Configuration - Cluster case .....	140
2.15.2 Remote Service .....	141
2.15.2.1 RSvP Remote Service (GEHCS only) .....	141
2.15.2.2 EDS Remote Service.....	145
2.15.3 Device Data.....	146
2.15.4 Contact Data.....	147
2.15.5 Service Tools Language (for Administrator).....	148
2.15.6 Time Settings.....	148
2.15.6.1 Date and Time menu .....	148
2.15.6.2 Time Server menu.....	149
2.15.7 Database Deletion Settings .....	150
2.15.7.1 Auto Delete settings.....	150
2.15.7.2 Delete option for worklist browser .....	151
2.15.8 Configuring SNMP .....	151
2.15.9 Platform Configuration.....	153
2.15.9.1 Licensing Preparation.....	153
2.15.9.2 Configuration Steps Summary.....	154
2.15.9.3 Platform configuration menu.....	154
2.15.9.4 Scalability setup menu .....	155
2.15.9.5 Integration configuration menu .....	156
2.15.10 Licensing Configuration.....	156
2.15.10.1 Preprocessing configuration menu.....	157
2.15.10.2 MailSender .....	157
2.15.10.3 CoLA License server .....	157
2.15.10.4 Floating License – Application licensing.....	160
2.15.10.5 Flexera licensing.....	162

---

2.15.11 Scalability- Clustered Servers.....	162
2.15.12 Audit Trail (EAT) .....	162
2.15.13 GIB Data .....	164
2.15.14 System Hardening .....	165
2.16 Job Card IST017 - Imaging Cockpit Components Installation .....	167
2.16.1 Loading the Imaging Cockpit Components .....	168
2.16.2 Installing the Imaging Cockpit Components .....	169
2.16.3 Activating the Web Client.....	171
2.17 Job Card IST009 - External Application(s) Installation .....	172
2.17.1 Foreword .....	172
2.17.1.1 Applications delivery and installation management changes .....	172
2.17.1.2 Product Hold warning notice example .....	173
2.17.1.3 Information about registration of installed configuration.....	173
2.17.1.4 Applications Software package content .....	174
2.17.2 Load the Application(s) from media.....	174
2.17.2.1 Using the Physical server's DVD drive .....	175
2.17.2.2 iLO DVD drive mapping - Remote loading on Physical Hardware Server .....	176
2.17.2.3 Virtual server and Physical server remote loading case .....	177
2.17.2.4 Loading Advanced Applications from USB device - eDelivery .....	178
2.17.3 Install the Application(s).....	178
2.17.4 Activate the Application(s).....	181
2.17.5 Applications Profile .....	182
2.17.5.1 Volume Viewer applications .....	182
2.17.5.2 Other Applications supported.....	183
2.18 Job Card IST010 - Administrative Configuration.....	184
2.18.1 Configuring DICOM hosts in Service Tools .....	184
2.18.2 Configuring DICOM Printers and Filmers .....	188
2.18.3 Configuring PostScript Printers.....	190
2.18.4 Users (EA3) (User account configuration) .....	191
2.18.4.1 Local User(s) Account Configuration .....	192
2.18.4.2 Configuring Enterprise User(s) Accounts.....	195
2.18.4.3 Assigning User Roles.....	197
2.18.5 Users (OS) Password Generation.....	198
2.18.6 Smart Card configuration .....	198
2.18.7 Client Timeout.....	203
2.18.8 Preprocessing Configuration.....	204
2.18.9 MailSender Settings .....	205
2.18.9.1 Configure the contact/recipient.....	209
2.18.10 End of Review .....	210
2.18.11 Certificate Management .....	211
2.18.11.1 Importing a certificate file to the AW Server trust store.....	212
2.18.11.2 Associating a certificate with feature(s).....	213
2.18.11.3 Exporting the AW Server certificate file to an external system .....	214
2.18.11.4 Renewing an expired external certificate .....	215
2.18.11.5 Renewing the AW Server certificate .....	215
2.18.12 AW Server declaration on DICOM images sources.....	219
2.18.12.1 DICOM Direct Connect integration .....	219
2.18.12.2 Imaging Cockpit / AW Server Web Client .....	220
2.18.13 Administrative Utilities .....	221
2.19 Job Card IST011 - Integration .....	221
2.19.1 Foreword .....	221

---

2.19.1.1 Integration modes supported with AW Server .....	221
2.19.1.2 Pre-requisite for Integration.....	223
2.19.2 Full front end integration (Hybrid): (3rdPartyIntegration) .....	224
2.19.2.1 Configuration steps on the AW Server .....	224
2.19.2.2 Configuration steps on the Universal Viewer .....	226
2.19.2.3 Configuration steps on the Client PC .....	228
2.19.3 Seamless Integration .....	228
2.19.3.1 Pre-requisites summary .....	228
2.19.3.2 Seamless integration - configuration steps on Universal Viewer Server.....	229
2.19.3.3 Seamless integration - configuration steps on AWS.....	230
2.19.3.4 Seamless integration - configuration steps on AWS, Service Tools.....	231
2.19.3.5 Seamless integration - configuration steps on Universal Viewer Client PC .....	236
2.19.3.6 Seamless integration - configuration steps on Image Sources.....	236
2.19.3.7 Seamless Integration - configuration checklist .....	236
2.19.4 DICOM Direct Connect integration .....	238
2.19.4.1 Pre-requisites.....	238
2.19.4.2 Configuration steps on AWS .....	238
2.19.4.3 Configuration steps on AWS, Service Tools .....	239
2.19.4.4 Configuration steps on the PACS/VNA/DICOM Remote Host .....	242
2.19.4.5 Configuration steps on the Client PC .....	243
2.20 Job Card IST012 - Virtual Servers Cluster Configuration .....	244
2.20.1 Foreword .....	244
2.20.2 Certificate Management .....	244
2.20.3 Scalability setup procedure.....	245
2.20.3.1 NTP server availability checks .....	245
2.20.3.2 Scalability setup.....	245
2.21 Job Card IST006 - Changing the Passwords.....	249
2.21.1 Passwords Change Procedure .....	250
2.21.1.1 Identify New Password(s) .....	250
2.21.1.2 Changing Linux passwords.....	251
2.21.1.3 Changing AW Server Users Password(s) .....	253
2.21.1.4 Changing Crypto Officer password and Master Encryption Key.....	255
2.21.1.5 Changing the default iLO User name and Password .....	255
2.21.2 Updating Password(s) in Connectivity Database.....	258
2.21.3 Communicate New Password(s).....	259
2.21.4 Performing a system backup .....	259
2.21.5 Password Form.....	259
2.22 Job Card IST013 - System Configuration Registration.....	259
2.22.1 Configuration registration steps.....	260
2.22.2 Process in case of issue at Registration time .....	262
2.22.2.1 In case of issue to access the AWCCT Website .....	262
2.22.2.2 In case of issue to get the registration key or to install it .....	263
2.23 Job Card IST014 - Server Installation Validation Tests .....	263
2.23.1 HealthPage Test.....	264
2.23.1.1 Required Tools .....	264
2.23.1.2 Procedure.....	264
2.23.2 Server Diagnostic Test .....	269
2.24 Job Card IST014A - Standard Client PC installation & Tests .....	270
2.24.1 Client Installation Procedure.....	270
2.24.1.1 Windows TM Client PC installation Procedure .....	270
2.24.2 Client (System) Test .....	274

---

2.24.2.1 Network Test (summary and client information).....	276
2.24.2.2 Validation Test Failure – What to do.....	279
2.24.2.3 Printing tests .....	280
2.24.2.4 Client Monitor screen resolution setup .....	281
2.24.2.5 AWS Client configuration for CPACS integration .....	281
2.24.2.6 AWS Client configuration for upgrade from AW Server 2.0 .....	282
2.25 Job Card IST014B - Seamless Client PC installation and Tests .....	282
2.25.1 Client Installation Procedure.....	282
2.25.1.1 Pre-requisites - Universal Viewer Client installation .....	282
2.25.1.2 AW Server Client Installation Procedure.....	282
2.25.1.3 Linux Client installation Procedure.....	284
2.25.2 Client (System) Test .....	284
2.25.2.1 Client Test (summary and client information) .....	285
2.25.2.2 Validation Test Failure – What to do.....	285
2.25.2.3 Printing tests .....	286
2.25.2.4 Client Monitor screen resolution setup .....	286
2.26 Job Card IST014C - Web Client Tests .....	286
2.27 Job Card IST015 - Final Settings .....	292
2.27.1 SNMP setup in iLO Service processor.....	292
2.27.1.1 Pre-requisite for using with Prodiag .....	292
2.27.1.2 SNMP setup in the iLO 5 service processor.....	292
2.27.1.3 Service Workflow .....	294
2.27.2 Anti-Virus setup .....	294
2.27.3 Scalability (cluster) mode operation verification .....	295
2.27.4 Hard disks serial numbers .....	295
2.27.4.1 At installation time.....	295
2.27.4.2 After hard disk drive replacement.....	295
2.27.5 PNF Firewall setting .....	296
2.27.6 Media Creator .....	296
2.27.7 Volume Viewer performances on VM.....	296
2.27.8 For China only - CFDA Registration documents.....	297
2.27.8.1 Installation on server.....	297
2.27.8.2 Upgrade.....	298
2.28 Job Card IST016 - System Handover to Customer .....	298
2.28.1 Installation handover tasks - Handover Checklist.....	298
2.28.2 Backup Parameters and Settings .....	301
2.28.2.1 Network and UPS configuration Backup .....	301
2.28.2.2 Configuration Backup.....	303
2.28.3 Final steps.....	304
2.28.3.1 AW Server User and IT Administration Training .....	304
2.28.3.2 GIB / SIEBEL update and paperwork .....	305
2.28.3.3 Register High Tier Server with Genpact .....	305
2.28.3.4 Capture the UDI number in Service Records .....	305
2.28.3.5 Print the AWS Configuration.....	306
2.28.3.6 Customer Release Note and information .....	307
2.28.3.7 HP Care Pack Warranty extension .....	307
2.28.3.8 PSI code verification .....	307
2.28.3.9 Site Cleanup .....	307
2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink .....	307
2.29.1 Installation/Upgrade Preparation .....	309
2.29.1.1 AW Server files preparation .....	309

---

2.29.1.2 Opening a console/terminal on the Edison HealthLink.....	309
2.29.2 AW Server Installation.....	310
2.29.2.1 Getting the MAC address and the network information for the AW Server Virtual Machine .....	310
2.29.2.2 Preparing the AW Server configuration with the Installation Wizard.....	310
2.29.2.3 Deploying the AW Server on a Virtual Machine .....	319
2.29.2.4 Displaying the AW Server Console .....	321
2.29.2.5 Configuring the HA Proxy for AW Server .....	323
2.29.2.6 Updating static routing file on AW Server.....	323
2.29.2.7 Allocating floating IP address for AW Server .....	324
2.29.2.8 Reviewing the network settings .....	326
2.29.2.9 Configuring the AW Server .....	327
2.29.3 AW Server Upgrade .....	335
2.29.3.1 Launching Service Tools.....	335
2.29.3.2 Navigating in Service Tools .....	338
2.29.3.3 Entering the Maintenance Mode .....	338
2.29.3.4 Backing up the configuration .....	341
2.29.3.5 Manual OS and AW Server Platform software upgrade.....	341
2.29.3.6 OS and AW Server Platform software Service Pack installation .....	349
2.29.3.7 Restoring the saved configuration .....	353
2.29.3.8 Restoring the integration.....	354
2.29.3.9 Restarting the RSvP Agent.....	355
2.29.4 Applications Installation/Upgrade .....	355
2.29.4.1 Loading the applications.....	356
2.29.4.2 Installing the applications .....	357
2.29.4.3 Activating the applications.....	358
2.29.5 AW Server final Settings.....	358
2.29.5.1 Security settings .....	359
2.29.5.2 Registering the system configuration .....	366
2.29.5.3 Backing up the configuration .....	368
2.29.5.4 Exiting maintenance mode.....	368
2.29.5.5 Accessing AW Server through HA proxy or external IP addresses.....	369
2.29.6 AW Server feature connection – CT Console.....	369
2.29.7 Installing the AW Server Client in MR Console.....	372
2.30 NanoCloud AW Server Installation in CT Console .....	373
2.30.1 Installation/Upgrade Preparation .....	374
2.30.1.1 Opening a console/terminal on the CT Console.....	374
2.30.1.2 AW Server files Preparation .....	375
2.30.1.3 Installation Tool files Preparation .....	376
2.30.1.4 Applications files Preparation .....	377
2.30.1.5 Service Pack file Preparation.....	378
2.30.1.6 Generating the eLicenses file .....	379
2.30.1.7 Copying the files prepared on the laptop into an USB media .....	380
2.30.2 AW Server Installation.....	381
2.30.2.1 Preparing and deploying the AW Server with the AW Server Installation Tool.....	381
2.30.2.2 Displaying the AW Server Console .....	390
2.30.2.3 Launching Service Tools.....	390
2.30.2.4 Configuring the AW Server with the Service Tools .....	394
2.30.3 AW Server Upgrade .....	399
2.30.3.1 Launching Service Tools.....	399
2.30.3.2 Entering the Maintenance Mode .....	402
2.30.3.3 Backing up the configuration .....	404
2.30.3.4 Preparing and deploying the AW Server with the AW Server Installation Tool.....	404
2.30.3.5 Displaying the AW Server Console .....	409

---

2.30.3.6 Launching Service Tools.....	410
2.30.3.7 Restoring the saved configuration .....	413
2.30.3.8 Restoring the integration.....	414
2.30.3.9 Restarting the RSvP Agent.....	415
2.30.4 AW Server Service Pack Installation .....	415
2.30.4.1 Launching Service Tools.....	416
2.30.4.2 Entering the Maintenance Mode .....	419
2.30.4.3 Backing up the configuration .....	421
2.30.4.4 Loading the OS and AW Server Platform software Service Pack .....	421
2.30.4.5 Installing the OS and AW Server Platform software Service Pack .....	423
2.30.5 Applications Installation/Upgrade .....	424
2.30.5.1 Launching Service Tools.....	424
2.30.5.2 Entering the Maintenance Mode .....	428
2.30.5.3 Loading the applications.....	430
2.30.5.4 Installing the applications .....	432
2.30.5.5 Activating the applications.....	432
2.30.6 AW Server final Settings.....	433
2.30.6.1 System Hardening.....	433
2.30.6.2 Changing the Passwords .....	434
2.30.6.3 Registering the system configuration .....	441
2.30.6.4 Backing up the configuration .....	443
2.30.6.5 Exiting maintenance mode.....	444
2.30.7 Installing AW Server Client on CT Console.....	444
<b>2.31 Secured for RMF mode .....</b>	<b>448</b>
2.31.1 RMF hardening package .....	448
2.31.2 AW Server Configuration and Limitations in Secured for RMF mode .....	448
2.31.3 Activating the Secured for RMF mode.....	451
2.31.3.1 Preparing the Secured for RMF mode.....	452
2.31.3.2 Executing the Hardening process .....	456
2.31.3.3 Finalizing configuration after Secured for RMF Mode activation.....	461
2.31.3.4 Interoperability with non-RMF compliant systems .....	462
2.31.3.5 Configuration registration solution in RMF (DoD) mode.....	465
2.31.3.6 Verifying the Secured for RMF Mode .....	466
2.31.4 Upgrading an AW Server in RMF mode .....	468
2.31.5 Installing Applications and Service Packs on AW Server in Secured for RMF mode .....	468
2.31.6 McAfee Virus Database update .....	469
2.31.6.1 Antivirus Database and engine update check .....	470
2.31.6.2 Antivirus Database Update.....	471
2.31.6.3 Antivirus Engine Update .....	474
2.31.7 Troubleshooting the Secured for RMF mode .....	476
2.31.8 Changing AW Server configuration in Secured for RMF mode .....	477
2.31.9 Account Authentication Policies .....	478
2.31.9.1 Linux Accounts .....	478
2.31.9.2 AW Server User Accounts.....	478
2.31.10 Local password policy in Secured for RMF mode .....	478
2.31.11 Checking RMF mode integrity.....	479
2.31.11.1 Checking integrity of the EAT related files .....	479
2.31.11.2 Checking integrity of the file system.....	479
<b>Chapter 3 Upgrade.....</b>	<b>481</b>
3.1 Foreword.....	481
3.2 Quick Start Installation Guide - Hardware Upgrade .....	482

---

3.3 Quick Start Installation Guide - Software Upgrade.....	483
3.4 Quick Start Installation Guide - Service Pack .....	486
3.5 Entering the Maintenance Mode.....	486
3.6 Scalability Upgrade .....	488
3.6.1 Adding an AW Server to an existing AW Servers Cluster.....	489
3.6.2 Removing an AW Server from an AW Servers Cluster.....	490
3.6.3 Upgrading an AW Server 3.0 Cluster to AW Server 3.2 release .....	490
3.6.4 Software Upgrade within an AW Servers Cluster .....	491
3.7 Hardware Upgrade .....	491
3.8 Applications Upgrade.....	491
3.9 System Configuration Restore Matrix .....	492
3.10 Job Card UPG001 - Software Upgrade.....	495
3.10.1 Upgrade Preparation - One week before the upgrade .....	496
3.10.1.1 Upgrade preparation - Perform Filesystem check.....	496
3.10.1.2 Upgrade preparation - Contact the IT Admin of the site .....	497
3.10.1.3 Floating License Server .....	497
3.10.1.4 Software Changes .....	497
3.10.1.5 Patients Image data backup .....	498
3.10.2 Verify that AW Server is operational.....	498
3.10.2.1 Check the hardware indicator LEDs (hardware server only) .....	498
3.10.2.2 Check the iLO Service processor (hardware server only) .....	498
3.10.2.3 Connect to the AW server .....	499
3.10.2.4 Important information about Hostnames.....	500
3.10.3 Backup the configuration .....	500
3.10.3.1 Backup the Network configuration.....	501
3.10.3.2 Backup the UPS configuration .....	502
3.10.3.3 Backup the Site configuration.....	503
3.10.3.4 Backup the PACS Integration configuration .....	504
3.10.3.5 Backup the existing exams status configuration.....	505
3.10.3.6 Backup the End of Review configuration.....	506
3.10.4 Software upgrade.....	506
3.10.4.1 Upgrade preparation for Virtual AW Server .....	506
3.10.4.2 Automatic OS and AW Server Platform software installation .....	508
3.10.4.3 OS installation .....	510
3.10.4.4 AW Server Platform software installation .....	517
3.10.4.5 OS and AW Server Platform software Service Pack installation .....	518
3.10.4.6 Imaging Cockpit Components installation .....	521
3.10.4.7 Loading the HPE R/T3000 UPS drivers and restoring the configuration (if applicable) .....	525
3.10.5 Reload and reinstall the Advanced Applications .....	526
3.10.5.1 Information about Volume Viewer Applications .....	526
3.10.5.2 Information about other Applications .....	526
3.10.5.3 Applications re-installation and upgrade process .....	526
3.10.6 Restore the Server configuration and licenses .....	527
3.10.6.1 Preliminary steps before restoration .....	527
3.10.6.2 Restoration steps .....	527
3.10.6.3 Licenses restoration.....	531
3.10.6.4 CardIQ Xpress Process (CXP) application reinstallation .....	531
3.10.6.5 Internal Applications restoration .....	531
3.10.7 RSvP connectivity re-installation .....	532
3.10.8 Integration restoration.....	532

---

3.10.9 Scalability restoration.....	533
3.10.10 Security settings.....	533
3.10.10.1 System Hardening.....	533
3.10.10.2 Passwords restoration .....	533
3.10.11 Register System configuration.....	533
3.10.12 Upgrade AW Clients after AW Server Upgrade .....	533
3.10.13 Final tests and system handover to customer.....	534
3.10.13.1 Final settings and System handover to customer.....	534
3.10.13.2 GIB / SIEBEL update and paperwork .....	534
3.10.13.3 Secure Media Destruction procedure .....	535
3.11 Job Card UPG002 - Scalability Upgrade .....	535
3.11.1 Adding an AW Server to an existing AW Servers Cluster.....	535
3.11.2 Removing an AW Server from an AW Servers Cluster.....	536
3.11.3 Software Upgrade within a Cluster .....	537
3.11.3.1 Pre-requisite for AW Server 3.0 upgrade case .....	537
3.11.3.2 AW Server 3.0 High Level Upgrade Procedure.....	538
3.11.3.3 AW Server 3.2 High Level Upgrade Procedure.....	541
3.12 Job Card UPG003 - Hardware Upgrade .....	543
3.12.1 Foreword .....	543
3.12.2 Old hardware checks .....	544
3.12.3 Old hardware configuration backup .....	544
3.12.4 New hardware installation - High level steps.....	544
3.12.5 System Configuration restoration .....	545
3.12.6 Patient data transfer .....	545
3.12.6.1 Check with customer what images can be deleted and proceed to deletion .....	546
3.12.6.2 De-activation of Auto-delete on the old AW Server.....	546
3.12.6.3 Change the IP address of the older AW server.....	547
3.12.6.4 Prepare the old AW Server for image transfer .....	548
3.12.6.5 Image transfer from old to new AW Server .....	548
3.12.6.6 Check installation of images on the new AW Server .....	550
3.12.6.7 Final steps on the new AW Server .....	551
3.12.6.8 Final steps on the old AW Server - Delete Patient data .....	551
3.12.7 Old hardware return procedure .....	553
3.13 Exiting the Maintenance Mode .....	553

## **Appendix A Appendices..... 555**

A.1 Overview.....	555
A.2 Specific field - Characters rules and limitations .....	555
A.3 Licensing.....	556
A.3.1 eLicense licensing.....	556
A.3.1.1 eLicense operation .....	557
A.3.1.2 Converting Node-Locked to Floating.....	563
A.3.2 Flexera Licensing.....	567
A.3.2.1 FlexNet Operations (FNO) .....	567
A.4 Maintenance Mode.....	571
A.4.1 Entering the Maintenance mode.....	571
A.4.2 Exiting the Maintenance mode.....	573
A.5 ClamAV® .....	575
A.5.1 Activating ClamAV® .....	576
A.5.2 Testing ClamAV® .....	578

---

A.5.3 Running ClamAV® manually .....	578
A.5.4 Checking ClamAV® status and logs .....	578
A.5.5 Managing an infection .....	579
<b>A.6 Software Loading Through iLO .....</b>	<b>579</b>
A.6.1 Foreword .....	579
A.6.1.1 Pre-conditions .....	580
A.6.1.2 Before you start.....	580
A.6.2 Starting the software load .....	580
A.6.2.1 Software load preparation with iLO 5 .....	580
A.6.2.2 Software load preparation with iLO 4, iLO 3 .....	584
A.6.2.3 Server reboot .....	587
A.6.2.4 Load From cold steps.....	588
A.6.2.5 Applications loading steps .....	588
A.6.2.6 Final step .....	588
<b>A.7 SNMP setup in the iLO service processor.....</b>	<b>588</b>
<b>A.8 Useful Commands and Tools.....</b>	<b>589</b>
A.8.1 Accessing the Terminal and login as root .....	589
A.8.2 Shutting down or rebooting the server .....	590
A.8.2.1 Through the Service Tools menu .....	590
A.8.2.2 Through command lines .....	591
A.8.3 Checking the routing table .....	591
A.8.4 Checking the Network settings .....	591
A.8.5 Checking the AWS configuration.....	591
A.8.6 Checking the OS release .....	591
A.8.7 Launching the Internet Navigator from the Server's KVM .....	591
A.8.8 DNS server(s) setup - Alternate method .....	594
A.8.8.1 Enter the Maintenance mode.....	595
A.8.8.2 Setup the DNS server(s) .....	595
<b>A.9 Filesystem Check.....</b>	<b>595</b>
A.9.1 Filesystem Check feature description.....	596
A.9.2 Filesystem check Side-effect "issue" description .....	596
A.9.3 Solutions to minimize the impact.....	597
<b>A.10 Hardware Return Procedure.....</b>	<b>599</b>
A.10.1 Old hardware removal .....	599
A.10.2 Old hardware return process.....	600
A.10.2.1 Return Procedure for Americas.....	600
A.10.2.2 Return Procedure for ASIA.....	600
A.10.2.3 Return address for Korea.....	601
A.10.2.4 Return address for Australia / New Zealand .....	601
A.10.2.5 Return address for GEMS.....	601
A.10.2.6 Return address for East Asia countries .....	601
A.10.2.7 Return procedure for other GEHC-Asia countries.....	601
A.10.2.8 Return Procedure for Europe .....	601
<b>A.11 Physical Servers - Installed Base .....</b>	<b>602</b>
A.11.1 AW Server - Product Description .....	602
A.11.1.1 The HPE ProLiant DL360 Gen9 Server low-tier rack-mount version .....	602
A.11.1.2 The HPE ProLiant DL360 Gen9 Server high-tier rack-mount version .....	602
A.11.2 Hardware Installation Verification .....	602
A.11.2.1 HPE ProLiant DL360 Gen9 Server Low Tier and High Tier Server hardware deliverables .....	603

# Chapter 1 Getting Started

## 1.1 Publication conventions

### 1.1.1 Intent of Information

This manual intends to address the following purposes:

#### **Chapter 2: New System Installation**

This chapter describes all the steps that the GEHC FE needs to do to install a new low-tier or high-tier AW Server system. It also describes how to install AW server(s) in a virtual environment. It is not intended to describe in detail the service tools, or any other process or tools used during installation.

#### **Chapter 3: Upgrade**

This chapter describes all the steps that the GEHC FE needs to do, to upgrade an AW Server to the latest current validated release.

It also describes how to add an AW Server to a cluster of AW servers.

It also describes how to upgrade an older AW Server hardware to a new AW Server hardware.

#### **Appendices**

These sections provide more detailed information about specific topics for reference

### 1.1.2 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.

### 1.1.3 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 <b>root</b>	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 <b>Enter</b> or Press <b>&lt;Enter&gt;</b>		This means you should press and release the "Enter" key on the keyboard.
Press <b>&lt;a&gt;</b>		This means you should press the "A" key on the keyboard in lowercase.
Press <b>Alt+C</b> or Press <b>&lt;Alt&gt; &lt;C&gt;</b>		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.

### 1.1.4 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.

### 1.1.5 Contents of this document

This document covers the installation and upgrade procedures of the AW Server 3.2 software.

It is not intended to cover the service procedures which are addressed in the AW Server 3.2 Advanced Service Manual 5771771-8EN, nor to cover the hardware installation which is addressed by the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware).

The following guide intends to summarize the installation instructions of a new AW Server 3.2 system, instructions that will be detailed all along this manual in the different sections / job cards of this chapter.

The installation / configuration instructions are applicable to the forward production physical servers delivered by GEHC (HPE ProLiant DL360 Gen10 Server), the Installed Base physical servers delivered by GEHC (HPE ProLiant DL360 Gen9 Server) and to the Virtual servers (the customer/client delivers and supports the hardware).

**NOTE**

For installed based physical servers deliverables, refer to [A.11 Physical Servers - Installed Base on page 602](#).

**NOTE**

Installation and Configuration of the Hypervisor environment for Virtual AW Server is under the customer/client's responsibility.

## 1.2 Access to Documentation and Service links

### 1.2.1 Documentation

#### 1.2.1.1 Access the AW Server 3.2 Service Documentation

The AW Server 3.2 Service Documentation is available **online** on:

- **Customer Documentation Portal** for basic Service Documentation:

<https://www.gehealthcare.com/documentationlibrary>

- **SIMS Content Viewer** for basic and advanced Service Documentation.

This information is available from the *AWS Service Tools* interface under the **Documentation** link.

It opens one new window with Service Documents information.

**NOTE**

For Chrome web browser user: A security setting blocks the opening of 2 new tabs simultaneously. It is an issue for ST Documentation part, because service guides and the user guides open on different pages. To allow the multiple page openings in Chrome, the FE should turn off pop up blocker.

**NOTE**

To view application documentation on a PC, you need Adobe® Reader® X or later. To download Adobe Reader, please visit Adobe System's website at [www.adobe.com](http://www.adobe.com).

#### 1.2.1.2 Navigating back and forth though cross-reference links in PDF files

To navigate through the previously/next visited page, you can use the following functionalities:

- You can use keyboard shortcuts as follows:
  - For previous view: Press simultaneously <Alt> and <Left arrow> keys.
  - For next view: Press simultaneously <Alt> and <Right arrow> keys.

OR

- You can add **Previous View** and **Next View** buttons to your Adobe Reader toolbar:
  - Click **View > Show/Hide > Toolbar Items > Page Navigation > Previous View / Next View.**
  - Use the **Previous View** and **Next View** buttons to navigate back and forth in the document.



**NOTE**

These functionalities work for most web browsers (FE Laptop or Client PC). However, they don't work for the Evince (AW/AWS pdf viewer) version installed on our platforms.

## 1.2.2 Service Web links

Service Web links are accessible under the Documentation menu:



## 1.3 Software Kit

### 1.3.1 Physical Software Kit

This section describes the content of the Physical Software Kit 5720614-23 (or higher). The following tables describe the media needed to install, upgrade, or update a Physical AW Server or a Virtual AW Server. The exact files needed, depending on the AW Server type (Physical, Virtual) and integration mode, are described in the relevant installation/upgrade sections of the Installation Manual.

**NOTE**

The reference checksums files (.sha256 extension) are not listed in these tables. However, they are present in the USB media to verify files integrity.

**NOTE**

In the tables below, the file names on the media have been written at the time of the creation of this manual. Thus, they may slightly differ.

**NOTE**

The Physical AW Servers are preloaded by Manufacturing with OS and AW Server software. So there is no media for initial installation.

**Table 1-1 AW Server 3.2 Software & Docs DVD**  - P/N: 5925050-2 (or higher)

Content	Purpose	AWS Type	Integration Mode
<i>aws-3.2-4.9-0.iso</i>	This iso file is used for <b>Initial installation &amp; Upgrade/Update</b> . It contains the AW Server software.	Virtual Physical	No-integ Hybrid Seamless DDC

**Table 1-2 Preinstalled OS and AW Server 3.2 Software and Docs**  - P/N: 5818084-10 (or higher)

Content	Purpose	AWS Type	Integration Mode
<i>aws-3.2-4.9-0.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) and the AWS software.	Virtual	DDC
<i>aws-3.2-4.9-0.vhdx.zip</i>	This compressed package is used for <b>Initial Installation &amp; Upgrade/Update</b> on Windows <b>Hyper-V</b> environment.	Virtual	DDC
<i>aws-3.2-4.9-0.qcow2.iso</i>	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.	Virtual	EHL NanoCloud
<i>startinstallwizard.bat</i> or <i>startinstallwizard.sh</i>	These scripts are used for <b>Initial Installation</b> to prepare the AW Server configuration (on Windows or on Linux).	Virtual	DDC EHL NanoCloud

**Table 1-3 AW Server 3.2 Full Software and Docs set**  - P/N: 5872674-6 (or higher)

Content	Purpose	AWS Type	Integration Mode
<i>AWS3.2_OS_7.2-Scientific-7.9.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) only.	Virtual	No-integ Hybrid Seamless
<i>AWS3.2_OS_7.2-Scientific-7.9.iso</i>	This iso file is used for <b>Upgrade/Update</b> . It contains the OS (Scientific Linux 7.9).	Virtual Physical	No-integ Hybrid Seamless DDC
<i>aws-3.2-4.9-0.iso</i>	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> . It contains the AW Server software.	Virtual Physical	No-integ Hybrid Seamless DDC

**Table 1-3 AW Server 3.2 Full Software and Docs set** - P/N: 5872674-6 (or higher) (Table continued)

Content	Purpose	AWS Type	Integration Mode
<i>aws-eml-1.12.0.iso</i>	These iso files are used for <b>Initial Installation &amp; Upgrade/Update</b> .	Virtual	No-integ
<i>aws-if-1.7.2.iso</i>	They contain the Imaging Cockpit Components:	Physical	Hybrid
<i>aws-ec-1.3.0.iso</i>	<ul style="list-style-type: none"> <li>• Edison Machine Light and Services</li> <li>• Imaging Fabric</li> <li>• Enterprise Cockpit Bundles</li> </ul>		DDC
<i>AW_Server_ED_Demo_Exams.iso</i>	This iso file contains the Demo Exams used to test the applications after installation.	Virtual Physical	No-integ Hybrid Seamless DDC EHL NanoCloud
<i>aws-3.2-4.9-0_src_dvd.iso</i>	This iso file contains the Open source license agreements (compliance with open source license terms).	Virtual Physical	No-integ Hybrid Seamless DDC EHL NanoCloud

## 1.3.2 Digital Software Kit

The AW Server 3.2 Digital Software Kit is compatible with electronic file delivery (eDelivery) and can be prepared on USB drive using the AW eDelivery Install Manager (AWeDIM) tool. The created USB drive can then be used to install the OS and Platform Software on Physical AW Server or on Virtual AW Server.

The following tables describe the files available to create the AW Server 3.2 Digital Software Kit. The exact files needed, depending on the AW Server type (Physical, Virtual) and integration mode, are described in the relevant installation/upgrade sections of the Installation Manual

### NOTE

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

**Table 1-4 AW Server SW for VM (p/n: 5921807-2ED / 5931189SSW)**

File name (in eDelivery Software Portal)	Purpose	AWS type	Integration Mode
<i>5865566-5_AW_Server_3.2_Ext.4.9_and_OS_OVA_Template_for_VM.ova</i>	<p>This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment.</p> <p>It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) and the AWS software.</p>	Virtual	DDC
<i>5865568-5_AW_Server_3.2_Ext.4.9_and_OS_VHDX_Template_for_VM.zip</i>	This compressed package is used for <b>Initial Installation &amp; Upgrade/Update</b> on Windows <b>Hyper-V</b> environment.	Virtual	DDC

**Table 1-4 AW Server SW for VM (p/n: 5921807-2ED / 5931189SSW) (Table continued)**

<b>File name (in eDelivery Software Portal)</b>	<b>Purpose</b>	<b>AWS type</b>	<b>Integration Mode</b>
5865570-5_AW_Server_3.2_Ext.4.9_and_OS_QCOW2_Template_for_VM.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.	Virtual	EHL NanoCloud
5865572-5_AW_Server_3.2_Ext.4.9_VM_Install_Wizard.zip	This compressed package is used for <b>Initial Installation</b> to prepare the AW Server configuration.	Virtual	DDC EHL
5940647-AW_Server_3.2_Ext.4.9_Install_Tool.zip	This compressed package is used for <b>Initial Installation</b> to prepare the AW Server configuration.	Virtual	NanoCloud
5865564-5_AW_Server_3.2_Ext.4.9_OS_Only_OVA_template_for_VM.ova	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment.  It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) only.	Virtual	No-integ Hybrid Seamless
5922981_AW_Server_3.2_Ext.4.9_Read_Me_First_Label.pdf	Information about how to get this Read Me First document. <b>Do not save this file on the AW system.</b>	Any	Any
packagemetadata.json	This file contains the reference checksums, of the files in this table, and additional data used by the remote download workflow.	Any	Any

**Table 1-5 AW Server SW (p/n: 5873501-5ED / 5931189SSW)**

<b>File name (in eDelivery Software Portal)</b>	<b>Purpose</b>	<b>AWS type</b>	<b>Integration Mode</b>
5865571-3_Operating_System_AWS3.2_OS_Rev.7.2_for_AW_Server_3.2.iso	This iso file is used for <b>Upgrade/Update</b> .  It contains the OS (Scientific Linux 7.9).	Virtual Physical	No-integ Hybrid Seamless DDC
5873503-5_AW_Server_3.2_Ext.4.9_Software_and_Docs.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> .  It contains the AW Server software.	Virtual Physical	No-integ Hybrid Seamless DDC
5865567-5_AW_Server_Edison_Machine_Light_and_Services_1.12.0.zip	These compressed packages are used for <b>Initial Installation &amp; Upgrade/Update</b> .	Virtual Physical	No-integ Hybrid DDC
5865565-5_AW_Server_Imaging_Fabric_Component_1.7.2.zip	It contains the Imaging Cockpit Components.		
5865569-5_AW_Server_Enterprise_Cockpit_Components_1.3.0.zip			
5922981_AW_Server_3.2_Ext.4.9_Read_Me_First_Label.pdf	Information about how to get this Read Me First document. <b>Do not save this file on the AW system.</b>	Any	Any

**Table 1-5 AW Server SW (p/n: 5873501-5ED / 5931189SSW) (Table continued)**

<b>File name (in eDelivery Software Portal)</b>	<b>Purpose</b>	<b>AWS type</b>	<b>Integration Mode</b>
<i>packagemetadata.json</i>	This file contains the reference checksums, of the files in this table, and additional data used by the remote download workflow.	Any	Any

## 1.4 Identification of Software releases

### Changes for CFDA rules

Identification of software releases shall comply with the CFDA regulations. Only the CFDA registered release number (I.e: aws-3.2- for AW Server 3.2) shall be displayed on the User Interface and on the software media art-work.

However, there is no change in the "conf" file and the SW media contains a "release.txt" file that displays the version in the usual way.

aws-3.2

This change also impacts the Applications and all the future products.

## 1.5 LOTO Warning

### CAUTION



Field Engineers must always adhere to the Lock Out Tag Out (LOTO) procedure when installing or servicing an AW Server. (Normally GEHC FEs are only responsible for servicing the ML350 (low tier) server; other server models are the responsibility of engineers from the respective hardware vendor).

Refer to the **AW Server 3.2 Advanced Service Manual** for the LOTO procedure.

## 1.6 Supported Web Browsers

AWS Web Client, Web Interface (a.k.a. Landing page) and Service Tools shall be compatible with desktop web browsers as follows:

	<b>AWS Web Client</b>	<b>Web Interface (a.k.a. Landing Page)</b>	<b>Service Tools</b>
Firefox compatible v54 and higher*	Compatible	Compatible	Compatible
Chrome compatible v86 and higher*	Compatible	Compatible	Compatible
MS Edge compatible v86 and higher*	Compatible	Compatible	Compatible
Safari compatible v10 and higher*	Compatible	Compatible	Not in scope and not verified
Internet Explorer 11.x*	Non-Compatible	Compatible with legacy format Web Interface	Compatible, <b>except</b> for <b>Web Client configuration</b> and <b>Register Configuration</b> pages

**NOTE**

\*Verify on latest release at time of verification.

# Chapter 2 Installation of a new AW Server

## 2.1 Overview

This chapter contains all information necessary for a GEHC field engineer (FE) to install a new AW Server hardware at a customer site

### **Pre-installation:**

- All preinstallation work must be completed before installing an AW Server system. Refer to the AW Server 3.2 Pre-Installation Manual for complete instructions.

### **GEHC hardware delivered AW Server:**

- All hardware installation work must be completed before loading and configuring a physical AW Server (hardware delivered by GEHC). Refer to the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware) for complete instructions.

### **Virtual AW Server:**

- All Hypervisor installation work must be completed by the IT administrator of the site before loading and configuring a virtual AW Server.

## 2.2 AW Server - Product Description

AW Server is a software package delivered with off-the-shelf, server-class hardware that allows easy selection, review, processing and filming of multiple-modality DICOM images from a variety of PC client machines via LAN or WAN networks. It also allows the user to choose lossless or lossy compression schemes to make a trade-off between speed and quality.

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

### 2.2.1 GEHC delivered AW Server hardware

Two hardware types of AW Server are currently available:

#### 2.2.1.1 The low-tier rack-mount version

Based on the HPE ProLiant DL360 Gen10 Server, it supports up to 40,000 slices at a time, depending upon which license is purchased.



#### 2.2.1.2 The high-tier rack-mount version

Based on the HPE ProLiant DL360 Gen10 Server, it supports up to 16,000, 40,000, 80,000 or up to 160,000 slices at a time, depending upon which license is purchased.

**Figure 2-1 HPE ProLiant DL360 Gen10 Server**

The customer's user interface is identical for all Low Tier or High Tier versions.

## 2.2.2 Hypervisor environments for Virtual AW Server

The virtual AW Server application is hypervisor agnostic and can be installed in the following hypervisor environments:

- VMware vSphere Hypervisor (ESXi) versions compatible with virtual machine hardware version 10. Refer to <https://kb.vmware.com/s/article/2007240>.
- Microsoft Windows Server Virtualization Generation 1 for Windows 10 (Hyper-V Gen1)

The hypervisor environment is not supplied by GEHC and installation / support is under the full responsibility of the customer.

## 2.2.3 The AW Server – system components

The three basic components in the AW Server system are:

1. The AW SERVER. This is the hardware foundation for the AW SERVER system, and is the direct responsibility of GEHC, including repair and/or replacement by vendors (HP) acting as agents of GEHC.
2. The NETWORK, which connects the AW Server to the clients, PACS, etc. The network is NOT the responsibility of GEHC.
3. The CLIENTS, which are provided by the customer. Other than installing client software on ONE customer PC, the clients are NOT the responsibility of GEHC.

## 2.2.4 Software Changes

The AW Server software may change from the time of this writing. If there is a discrepancy between this document and the screens you see, use your best judgment to complete this procedure as it was originally intended.

## 2.2.5 Before you start

Before starting the installation, verify that at minimum, the following system information is available.

It can be obtained from the site's network administrator, or from the Site Survey information documented by the vendor FE during pre-installation.

- Hostname
- Server IP address
- Gateway IP address
- Service processor IP address and password (if applicable)
- Proxy configuration

- LDAP server configuration, if EA3 authentication server is used for the site
- Domain name (if applicable for the site)

**NOTICE**

In Seamless integration with the GE PACS, the AW Server and the Universal Viewer PACS server must be on a trusted network. If encryption is required for client-server communication using HTTPS, set it at system level via the Universal Viewer Site Configuration Tool. Refer to the Universal Viewer Installation Manual.

## 2.2.6 Software preload by Manufacturing

### 2.2.6.1 GEHC delivered Physical servers

The Physical AW Servers (hardware delivered by GEHC) are preloaded by Manufacturing with Linux Operating System (OS), AW Server Platform software and UPS drivers (if applicable).

The hardware types currently preloaded are:

- HPE ProLiant DL360 Gen10 Server Low Tier
- HPE ProLiant DL360 Gen10 Server High Tier

The below label is affixed to the AW Server packaging.



### 2.2.6.2 Virtual AW Servers on customer's physical servers

Virtual AW Servers cannot be preloaded by Manufacturing.

The AW Server platform software and the Applications shall be loaded on the Virtual Machine (VM), once it has been created by the IT administrator of the site through the OS Template (OVF) delivered by GEHC.

## 2.3 Quick Start Installation Guide - Physical AW Server

The following guide intends to summarize the installation instructions of a new AW Server 3.2 system, instructions that will be detailed all along this manual in the different sections / job cards of this chapter.

- The following installation / configuration instructions are applicable to physical servers delivered by GEHC (Forward Production HPE ProLiant DL360 Gen10 Server).
- The following instructions are not applicable to virtual servers (the customer delivers and supports the hardware). For virtual server installation, refer to [2.4 Quick Start Installation Guide - Virtual AW Server on page 35](#).

**NOTICE**

In case the physical server would not have been preloaded in Manufacturing (I.e: due to manufacturing no able to proceed at that time), jump to sections [2.5 Job Card IST001A - Hardware Installation Verification on page 45](#) and [3.10 Job Card UPG001 - Software Upgrade on page 495](#) to perform a load from cold. Bypass backup and restore related sub sections.

**NOTE**

This manual does not address the hardware installation which is covered by the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware).

Physical servers (HPE ProLiant DL360 Gen10 Server hardware delivered by GEHC) are preloaded in Manufacturing.

### 2.3.1 Physical AW Server Characteristics

Available configurations for physical AW Server.

**Table 2-1 Low Tier Physical Machine characteristics**

HW platform	Processor	RAM	Users	Slice count license	No-Integ (Stand-alone AW Server)	Hybrid	DICOM Direct Connect (DDC)
HP DL360 – G10	20 CPUs	96GB	10	40K slices (SdC_Low_Tier_Premium)	X*	X*	

\*Imaging Cockpit supported.

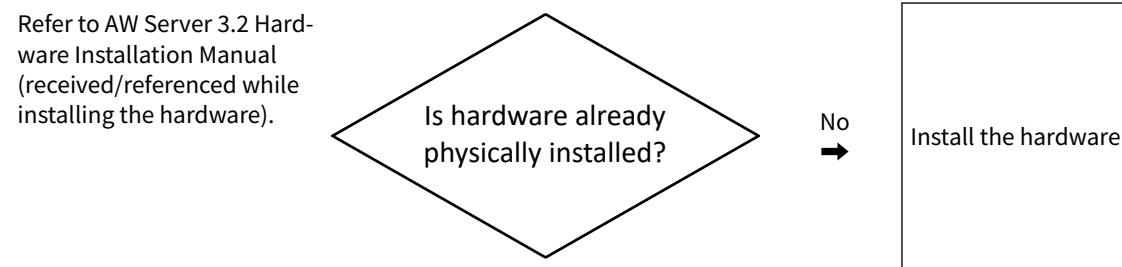
**Table 2-2 High Tier Physical Machine characteristics**

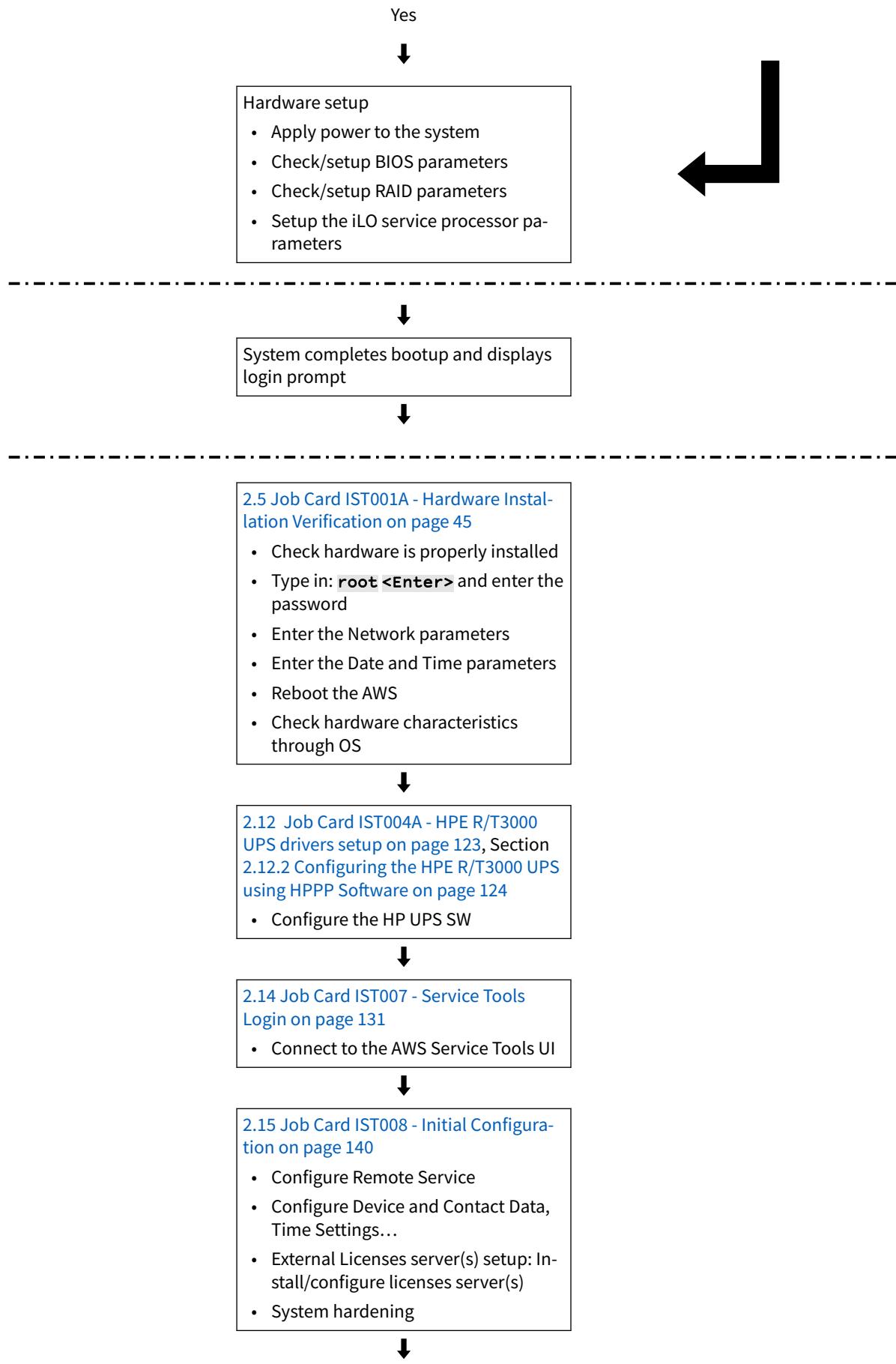
HW platform	Processor	RAM	Users	Slice count license	No-Integ (Stand-alone AW Server)	Hybrid	DICOM Direct Connect (DDC)
HP DL360 – G10	36 CPUs	384GB	50	80K slices (SdC_High_Tier_Standard)	X*	X*	X*
	36 CPUs	384GB	50	160K slices (SdC_High_Tier_Premium)	X*	X*	X*

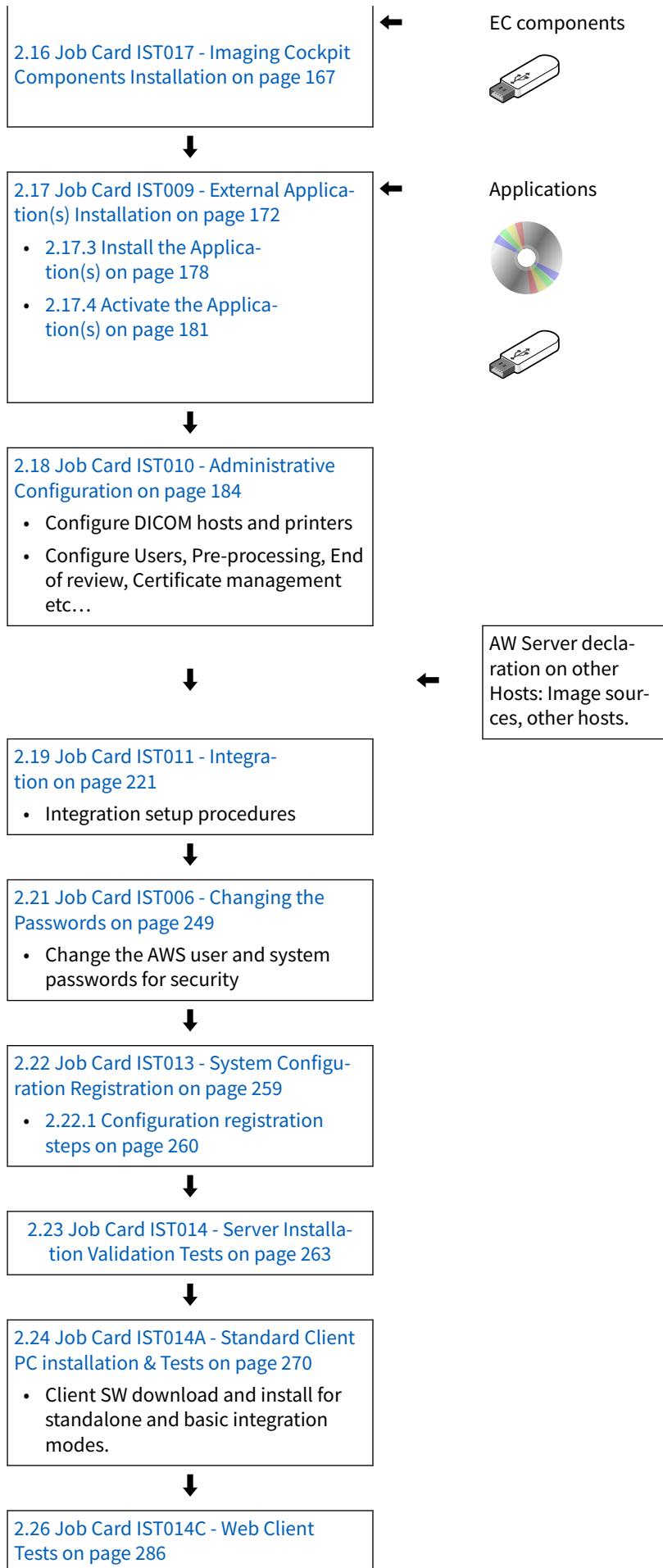
\*Imaging Cockpit supported.

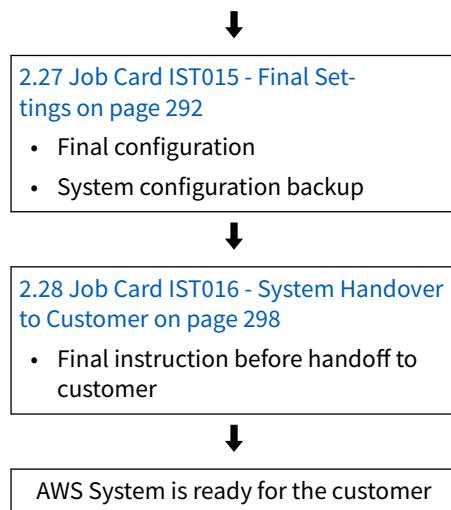
### 2.3.2 Physical AW Server Installation steps overview

Installation / Configuration flowchart for preloaded physical AW Server:









## 2.4 Quick Start Installation Guide - Virtual AW Server

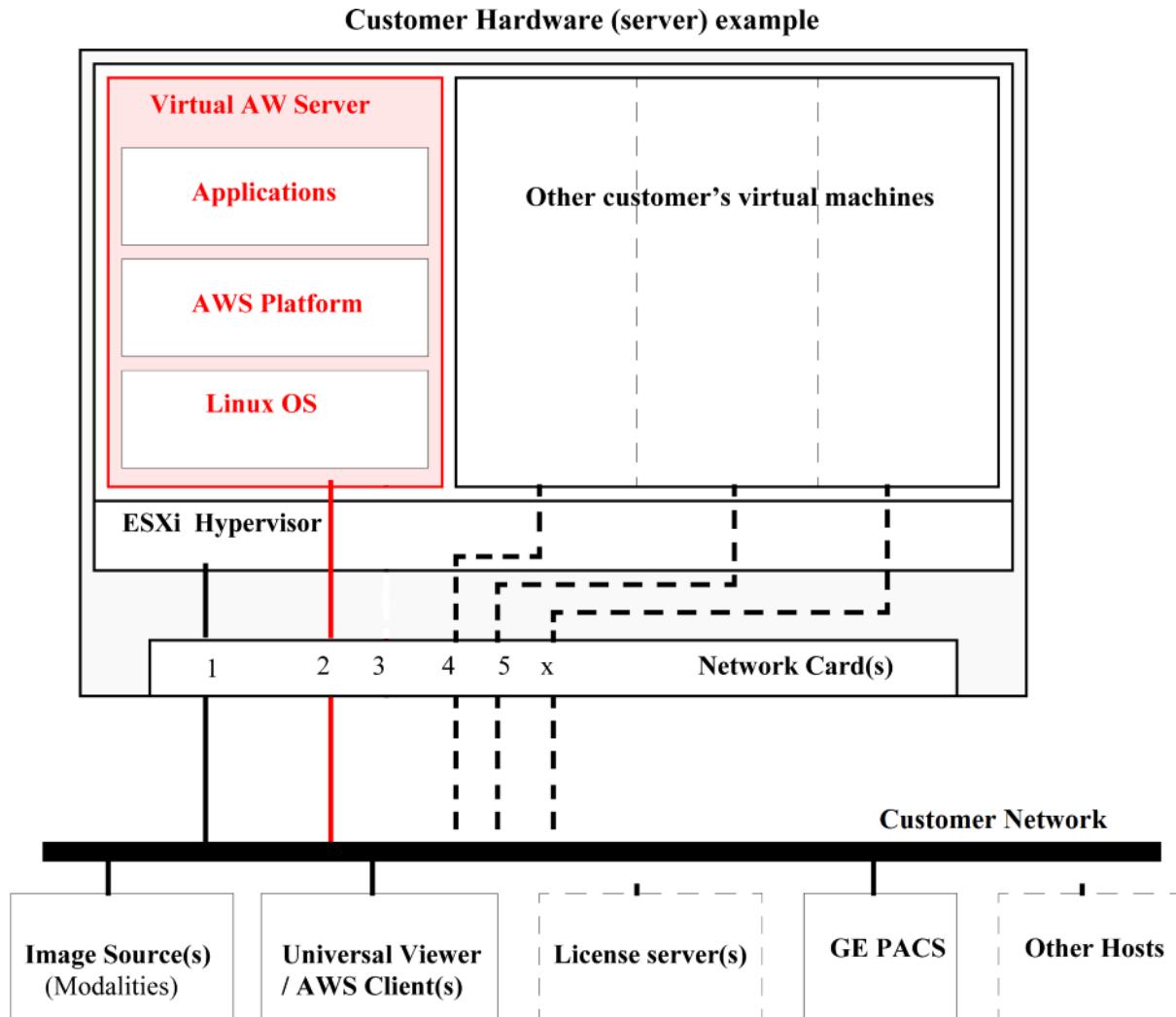
### NOTE

For the AW Server integrated within the CT/MR Console Environment (Edison HealthLink or CT Console), refer to [2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink on page 307](#) or [2.30 NanoCloud AW Server Installation in CT Console on page 373](#).

For virtual AW servers, the customer delivers and supports the hardware, and creates the VM (virtual machine) on which the virtual AW Server is hosted).

- Section [2.4.2 Virtual AW Server Installation steps overview on page 38](#) : Installation of a virtualized AW server (AW Server is installed on a customer's server as a virtual machine).
- Section [2.4.3 Quick Start Installation Guide - Scalable Virtual servers on page 42](#) : Installation of a cluster of virtualized AW server (scalability)

A cluster of Virtual AW servers (also called Scalability) is a set of several AW Servers (currently up to 75), which form a "bigger - more powerful" AW Server, that can be accessed with appropriate performances by more AW Server Clients (PCs).



### NOTICE

Installation and Configuration of the Hypervisor environment for Virtual Servers is under the Customer's responsibility.

### NOTE

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

## 2.4.1 Virtual AW Server Characteristics

Hosted OS requirements - Minimum resources to run each AW Server Node - Available configurations for virtual AW Server.

**Table 2-3 Low Tier Virtual Machine characteristics**

<b>Pro- cessor</b>	<b>Virtu- al HDD</b>	<b>RAM</b>	<b>NIC</b>	<b>Users</b>	<b>Slice count license</b>	<b>No-In- teg (Stan- da- lone AW Ser- ver)</b>	<b>Hy- brid</b>	<b>Seam- less</b>	<b>DI- COM Direct Con- nect (DDC)</b>	<b>DDC in Edi- son Healt hLink</b>	<b>DDC in CT Nano- Cloud</b>
8 vCPUs	210GB	24GB	1	10	8K slices (SdC_Server_Two_Seats)	X	X				
8 vCPUs	210GB	24/32 GB*	2	25	16K slices (SdC_Server_Four_Seats)			X			
8 vCPUs	210GB	64GB	1	25	40K slices (SdC_Low_Tier_Premium)			X			
8 vCPUs	210GB	64GB	1	10	40K slices (SdC_Low_Tier_Premium)	X	X		X		
8 vCPUs	210GB	96 GB**	1	10	40K slices (SdC_Low_Tier_Premium)	X	X		X		
8 vCPUs	70GB	64GB	1	1	40K slices (SdC_Low_Tier_Premium)					X	
8 vCPUs	70GB	12GB	1	1	4K slices (Sdc_Nano_4K)						X
8 vCPUs	70GB	26GB	1	1	12K slices (Sdc_Nano_12K)						X
8 vCPUs	70GB	32GB	1	1	16K slices (Sdc_Nano_16K)						X

\*For Seamless 24GB minimum, 32GB is recommended.

\*\*96GB for Imaging Cockpit support.

**Table 2-4 High Tier Virtual Machine characteristics**

<b>Pro- cessor</b>	<b>Virtu- al HDD</b>	<b>RAM</b>	<b>NIC</b>	<b>Users</b>	<b>Slice count license</b>	<b>No-In- teg (Stan- da- lone AW Ser- ver)</b>	<b>Hy- brid</b>	<b>Seam- less</b>	<b>DI- COM Direct Con- nect (DDC)</b>	<b>DDC in Edi- son Healt hLink</b>	<b>DDC in CT Nano- Cloud</b>
24 vCPUs	210GB	64GB	1	30	40K slices (SdC_Server_Eight_Seats)	X	X				
24 vCPUs	210GB	72GB	1	50	40K slices (SdC_Server_Eight_Seats)	X	X				
24 vCPUs	210GB	104GB *	1	50	40K slices (SdC_Server_Eight_Seats)	X	X		X		

**Table 2-4 High Tier Virtual Machine characteristics** (Table continued)

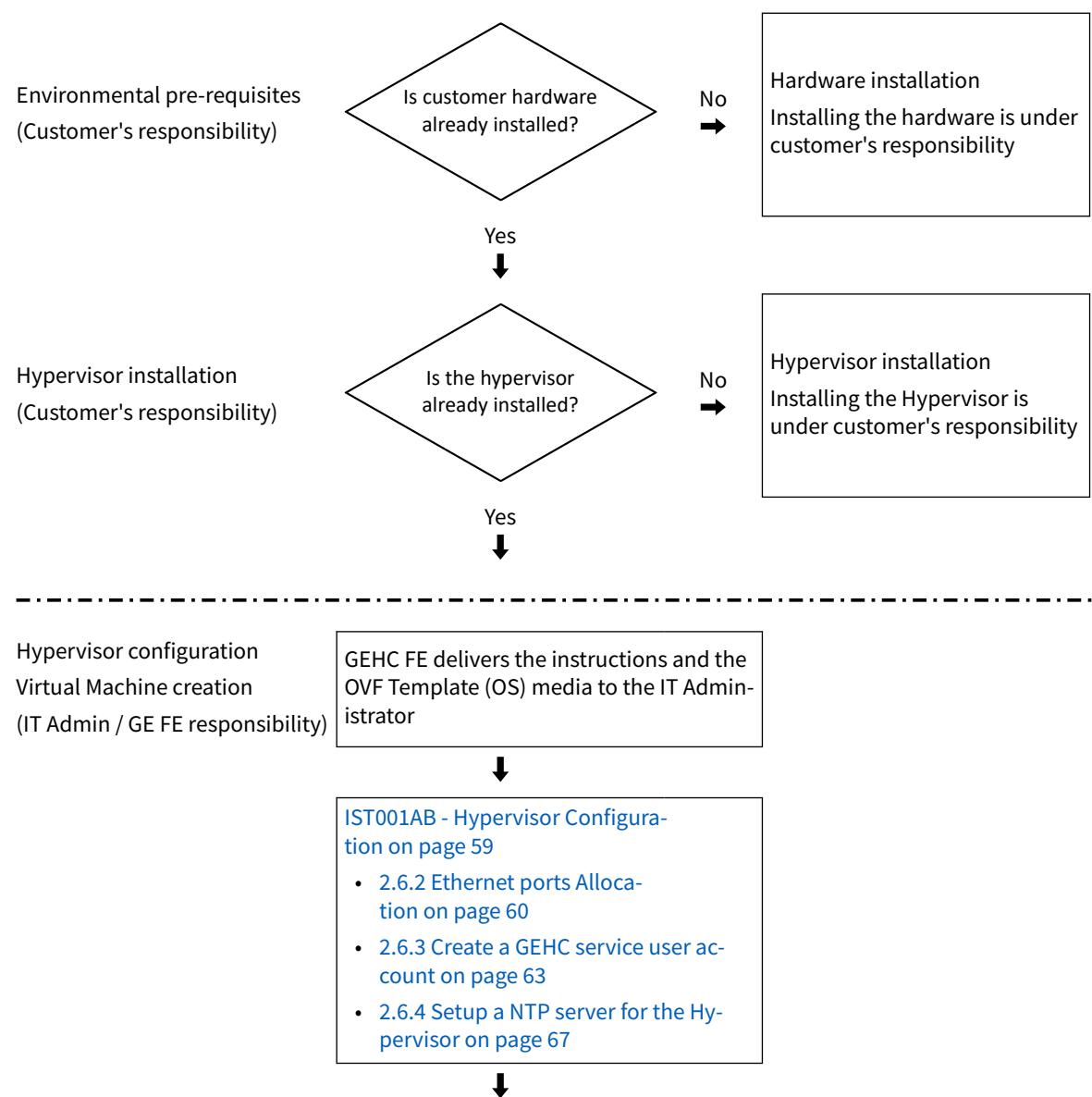
Processor	Virtual HDD	RAM	NIC	Users	Slice count license	No-Integ (Standalone AW Server)	Hybrid	Seamless	DI-COM Direct Connect (DDC)	DDC in Edison HealthLink	DDC in CT Nano-Cloud
24 vCPUs	210GB	64GB	1	50	40K slices (SdC_Server_Eight_Seats)			X			

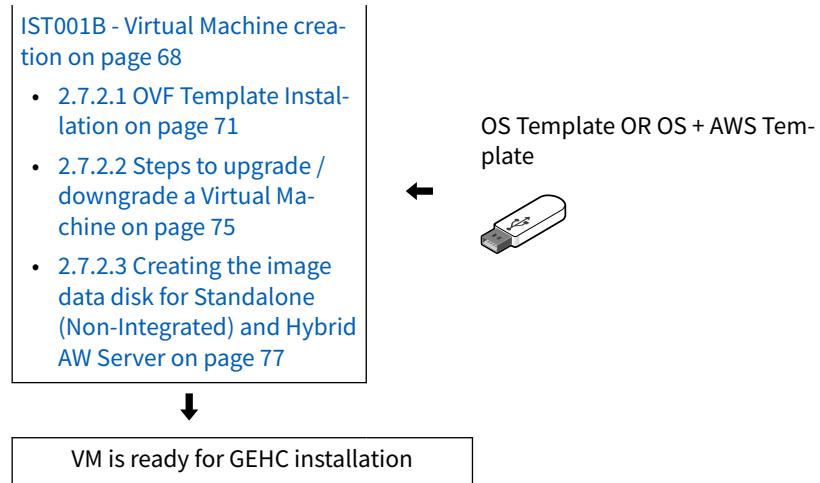
\*104GB for Imaging Cockpit support.

For No-Integ (Standalone AW Server) and Hybrid integration, an additional disk for image/backup is required (300GB min - 6TB max).

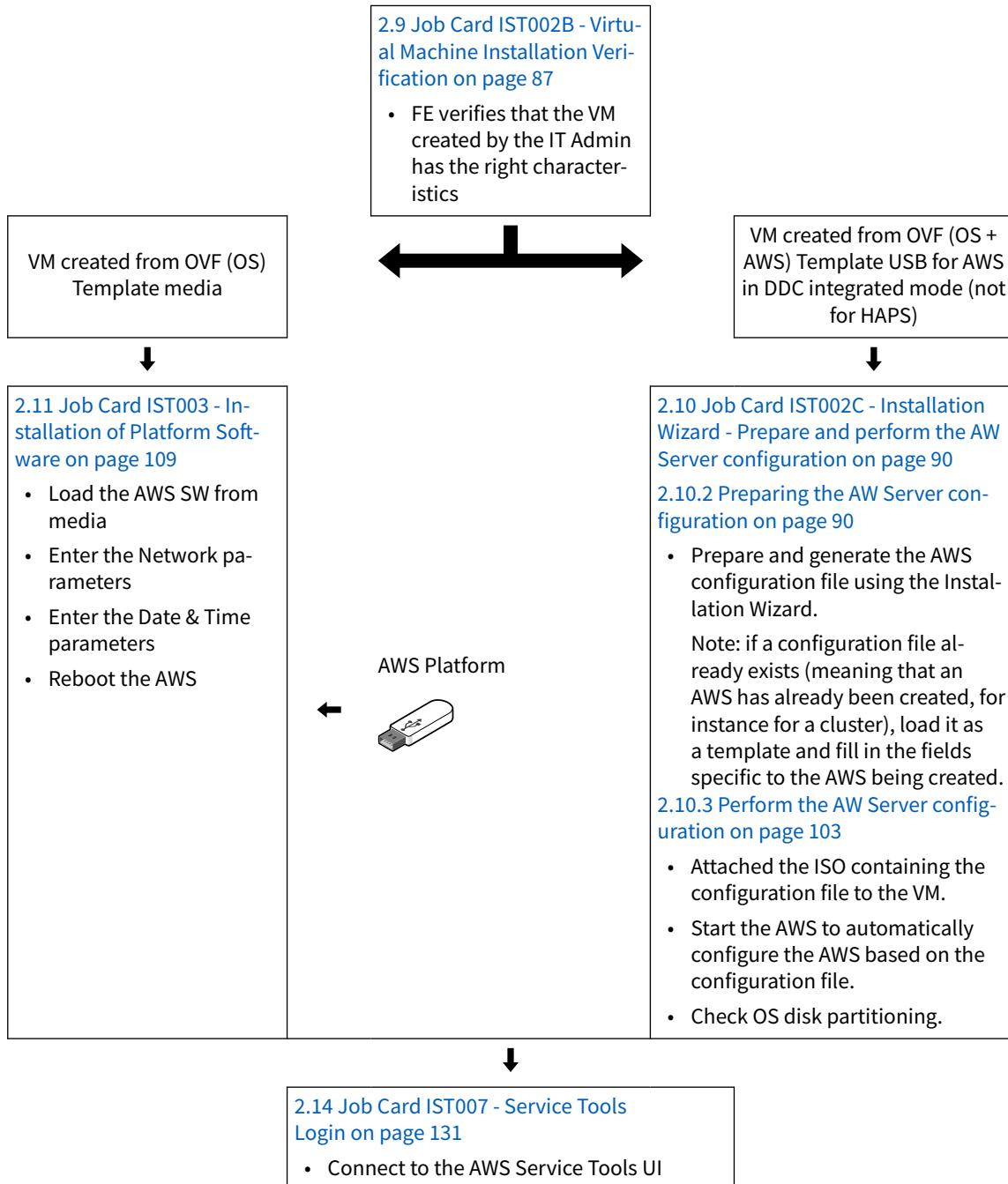
## 2.4.2 Virtual AW Server Installation steps overview

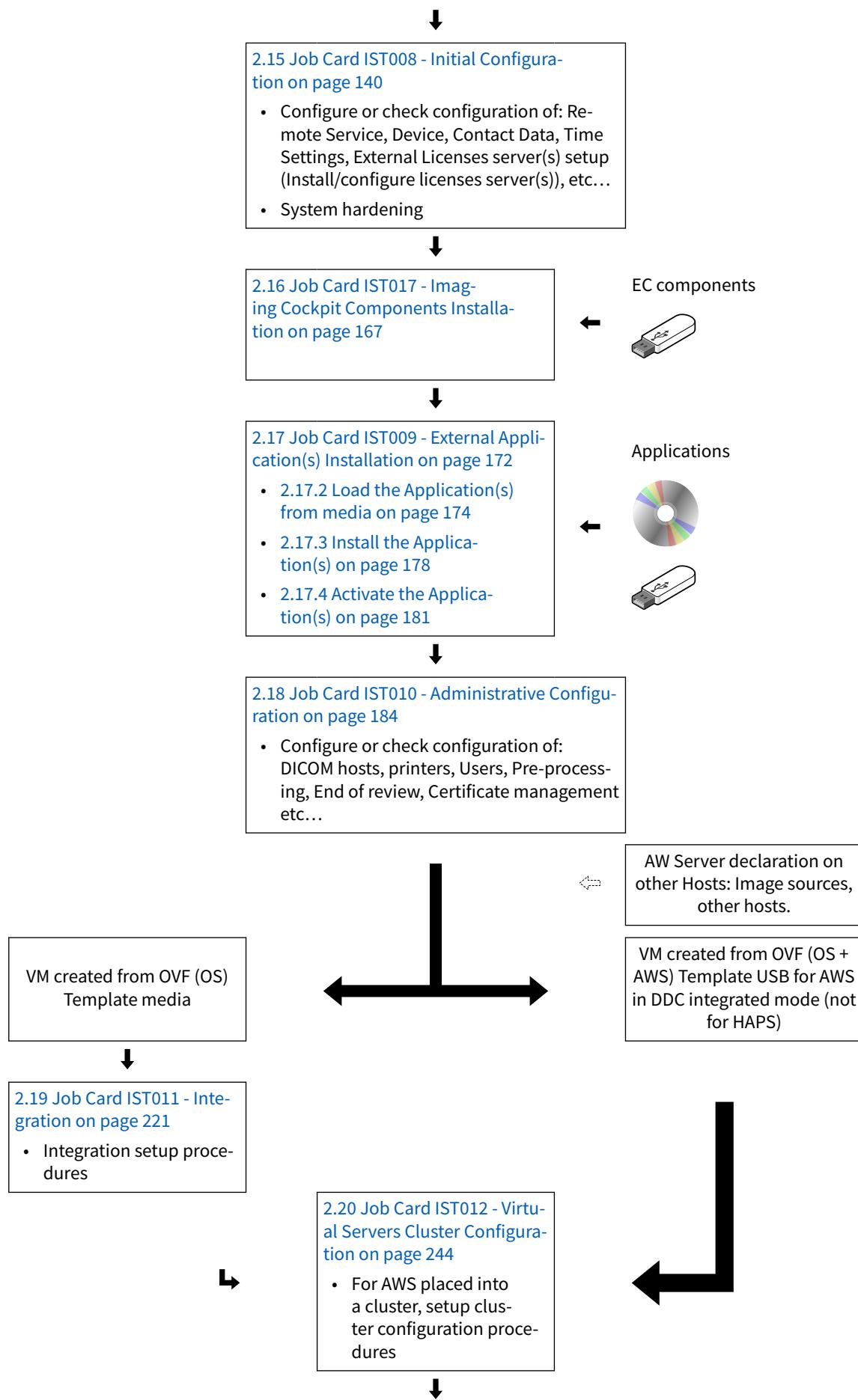
Section performed by the IT Administrator of the site.

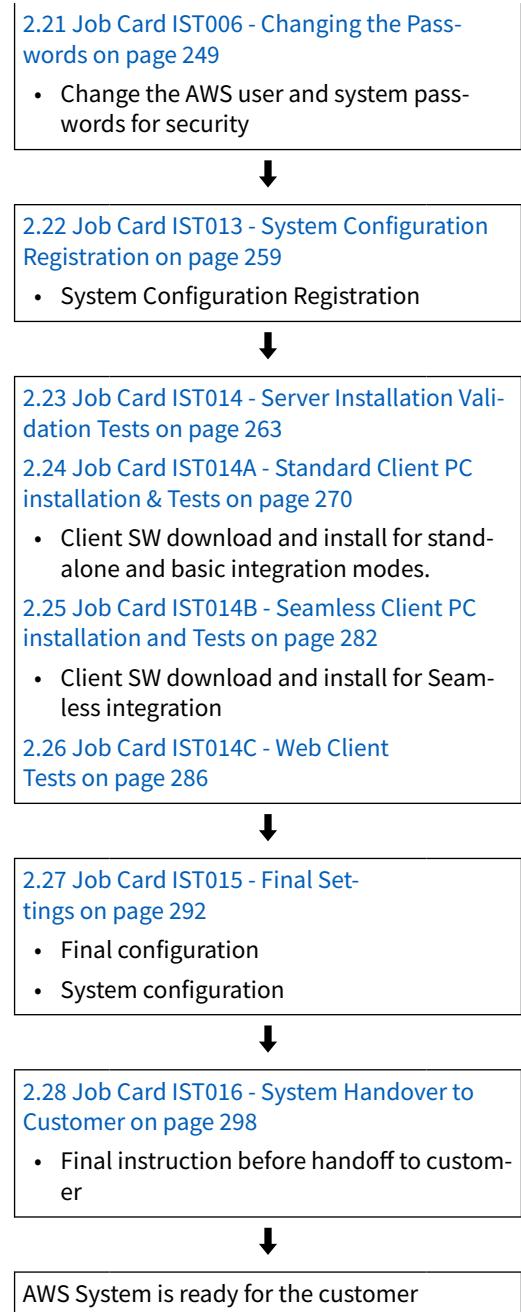




Section performed by the GEHC FE.



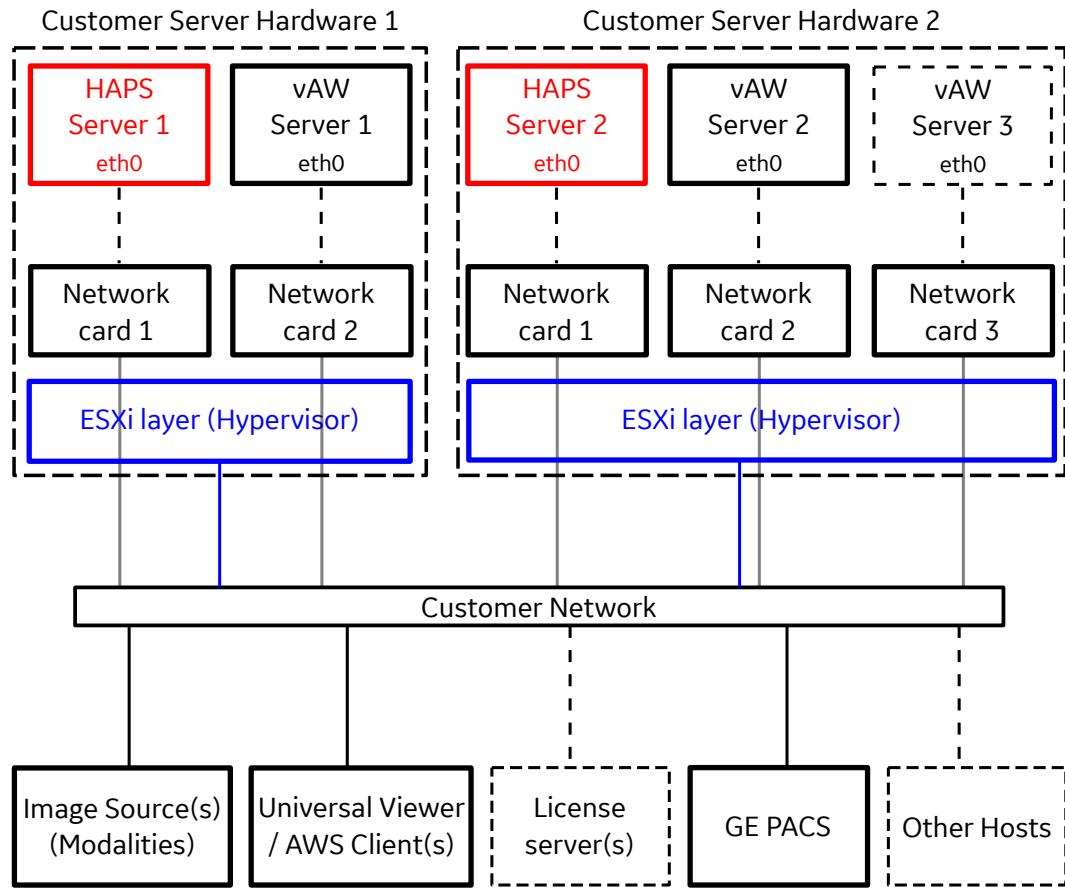




## 2.4.3 Quick Start Installation Guide - Scalable Virtual servers

### AW Servers scalability overview

Figure 2-2 Example of a cluster of 3 virtual AW Servers using 2 customer's hardware servers



#### The virtual AW Server system provides a scalability function:

Several virtual AW Servers can be grouped in a cluster. The cluster can be distributed on several hospitals (the second hardware can be in another hospital). In a cluster, the AW Servers can be connected to provide more computing power to the users.

An AW Server which is part of a cluster is called a node.

#### NOTE

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

#### NOTICE

Two HAPS (High Availability Preferences Sharing) servers VM shall be created through the OVF Template OS and the AWS Platform software.

## Current Scalability Limitations

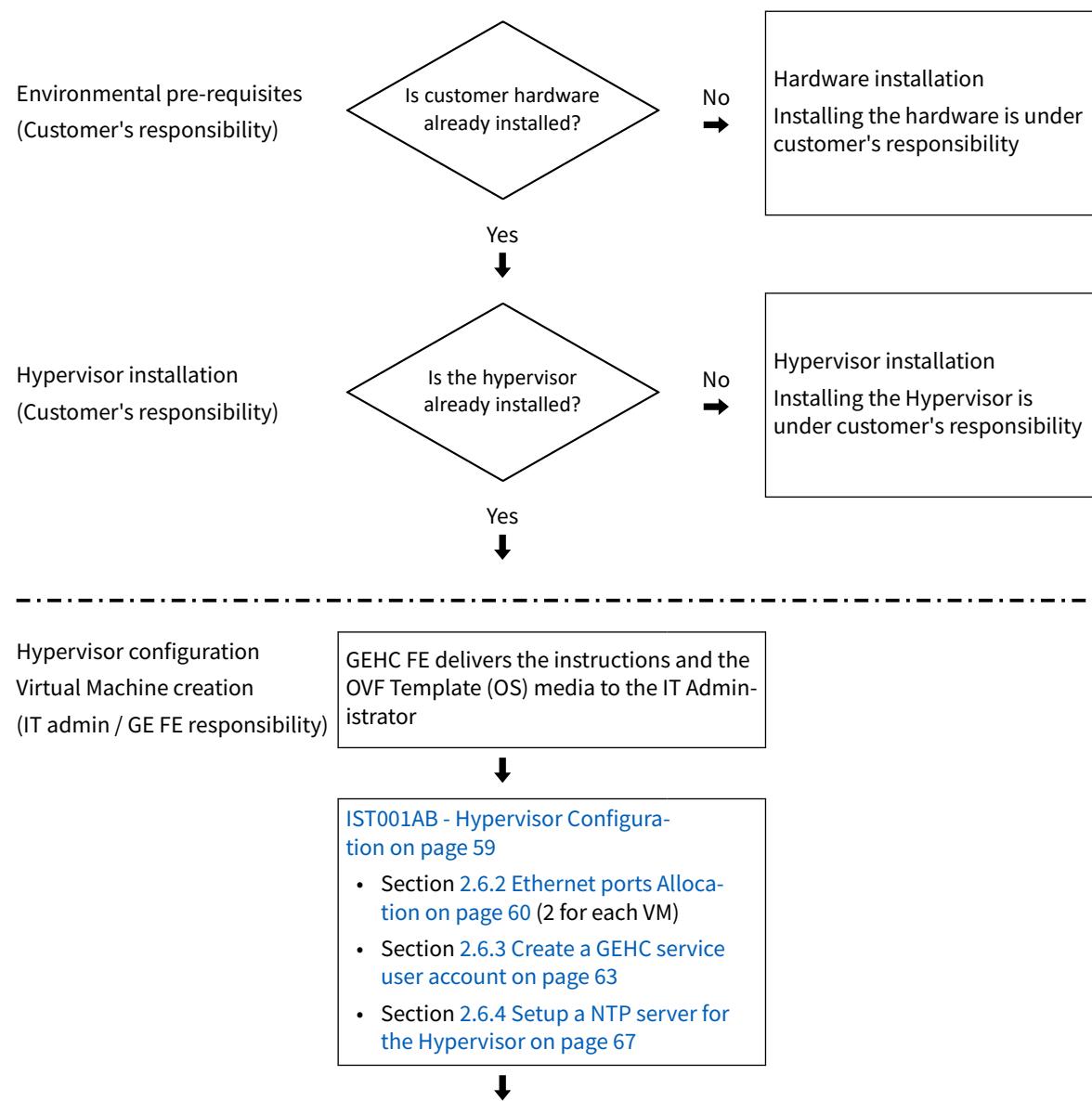
- Scalability is currently only supported on Virtual AW servers and limited to a maximum of seventy five (75) virtual AW Servers 16K slices (AW Server 40K slices is supported in cluster mode only for DICOM Direct Connect integration).
- Each virtual AW Server must be linked to one dedicated physical 1Gb network card.
- For proper Scalability operation, all AW Servers in the cluster must be linked to the Hospital network to ensure communication with the DICOM hosts, the Universal Viewer / AWS Client and the PACS, etc.), and to ensure communication between the nodes of the cluster (each virtual AW server).

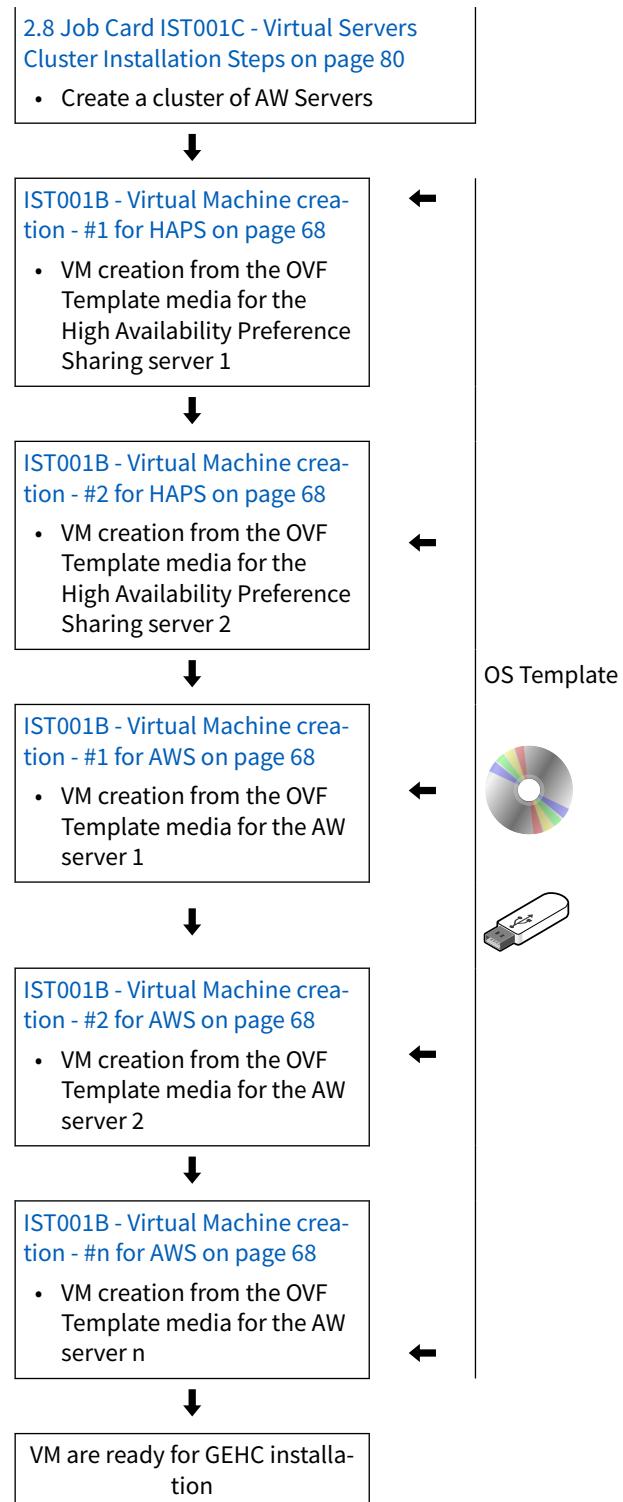
### NOTICE

To ensure high availability, the two HAPS servers shall preferably be hosted on two different hypervisors.

## Scalable AW Servers Installation steps overview

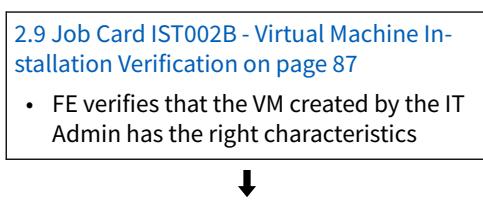
Section performed by the Customer IT Admin.

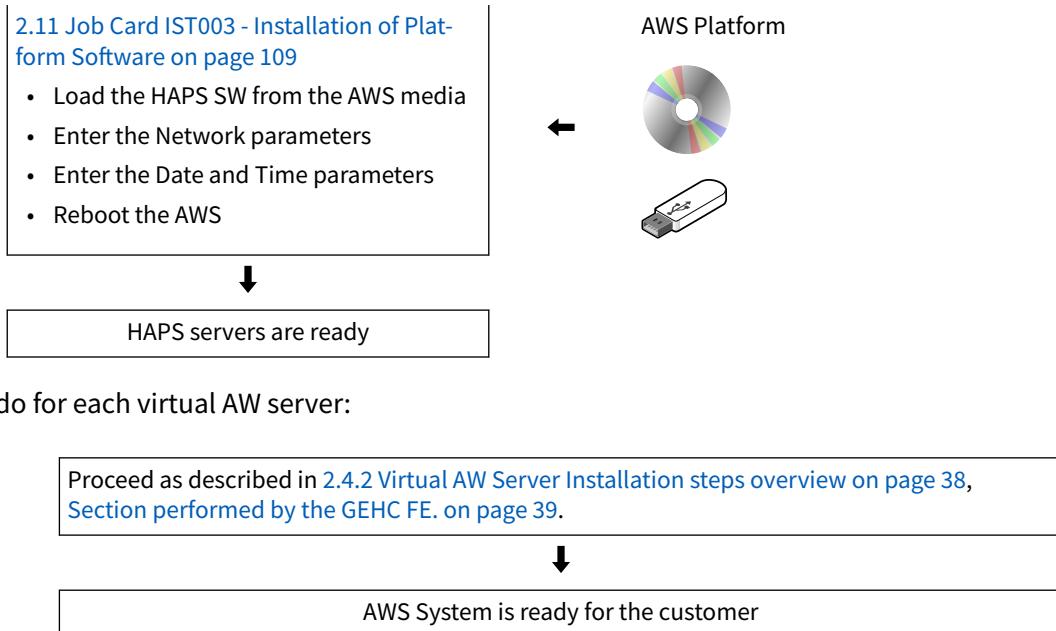




Section performed by the GEHC FE.

To do for each virtual HAPS server:





## 2.5 Job Card IST001A - Hardware Installation Verification

This Job Card applies to all GEHC hardware delivered servers.

### NOTICE

#### \*\*\* IMPORTANT PROCESS REQUIREMENT \*\*\*

Any deficiencies or hardware failures found while executing the following verification process must be IMMEDIATELY reported to the GEHC OLC support team, and the Vendor PMI (Installation Manager) and or Vendor FE to be resolved prior to GEHC Service accepting ownership of the system, and installing the AW Server software!!!

Training time can be logged if the GEHC FE desires to observe – but not actual installation time until the hand-off is successful.

### NOTE

This Job Card describes the installation verification for the forward production server (HPE ProLiant DL360 Gen10 Server).

For installed based physical servers deliverables, refer to [A.11 Physical Servers - Installed Base on page 602](#).

### 2.5.1 Time Reporting for Installation and Warranty

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

- HP High Tier server- 8 to 11 hours, with:
  - 5 to 6 hours for the PHYSICAL installation
  - 3 to 5 hours for the AWS Software / Configuration (GEHC) installation.
- HP Low Tier server- 4 to 7 hours, with:
  - 1 to 2 hours for the PHYSICAL installation

- 3 to 5 hours for the AWS Software / Configuration (GEHC) installation.

Charge any additional time to the appropriate service class. Examples include: "TRAINING" (87), "Installation Support" (04) and Customer Courtesy Call (90).

Charge any system malfunction / troubleshooting and repair time to the appropriate warranty service class (10 or 11).

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

## 2.5.2 Hardware Installation validation

### 1. Supplies

- High Tier Server or Low Tier Server
- UPS option (if applicable)
- KVM option (if applicable) or Monitor, Keyboard and Mouse
- Power cables, Network cables and video cable for KVM
- Network switch option (if applicable)
- PDU (Power Distribution unit) option (if applicable)

### 2. Tools and parts required

- AW Server platform software media.
- AW Server OS media: To be used at time of first installation (or needed if load-from-cold is required), if the system has not been Preloaded by Manufacturing.
- UPS drivers CD (for UPS option if applicable): (needed if load-from-cold is required).
- GEHC service (FE) laptop and network cable.

### 3. Pre-requisites

The High Tier server and accessories may have been physically installed by the IT department of the site. Verify that all of the following steps have been completed correctly:

- Server securely mounted in rack (if applicable).
- If applicable, PDU option is securely mounted in rack.
- If applicable, UPS option is securely mounted in rack.
- If applicable, KVM option is securely mounted in rack.
- If applicable, Network Switch option is securely mounted in rack.
- All necessary power cables are installed.
- All necessary network cables are installed.
- If applicable, the UPS shutdown line USB cable is installed between the server and the UPS.
- If applicable, KVM option connected or Monitor, Keyboard and Mouse.

For HPE ProLiant DL360 Gen10 Server Low Tier and High Tier, see [2.5.3 HPE ProLiant DL360 Gen10 Server High Tier and Low Tier on page 46](#).

## 2.5.3 HPE ProLiant DL360 Gen10 Server High Tier and Low Tier

1. Verify that the Server hardware inventory (provided within server documentation) includes the items below:

- For HPE ProLiant DL360 Gen10 Server High Tier:

Description	Quantity
HP DL360 chassis	1
300GB 15K SAS 2.5" HDD	2
1.8TB 10K SAS 2.5" HDD	6
Internal DVD+/-RW drive	1
Internal RAID controller	1
Redundant hot-swappable AC power supply	2
Tool-less slide rail kit	1

- For HPE ProLiant DL360 Gen10 Server Low Tier:

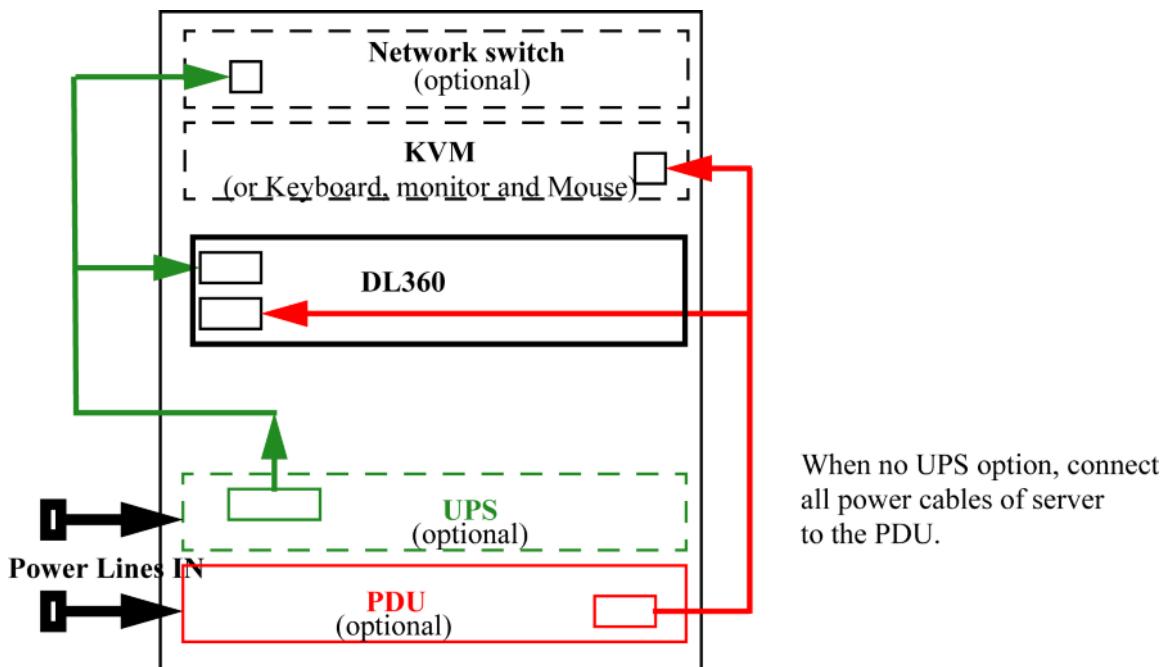
Description	Quantity
HP DL360 chassis	1
300GB 15K SAS 2.5" HDD	2
600GB 10K SAS 2.5" HDD	6
Internal DVD+/-RW drive	1
Internal RAID controller	1
Redundant hot-swappable AC power supply	2
Tool-less slide rail kit	1

2. Verify that the server slides out and in the rack enclosure easily, and do not bind or cause disconnected cables. This means that the cables, and cable arm harness (if installed) must be dressed and strain-relieved properly.
3. Inspect all units to insure that there is no visible chassis damage.
4. Verify that the server has two 300GB drives and six 1.8TB drives (High Tier) or six 600GB drives (Low Tier), as shown in the picture below:



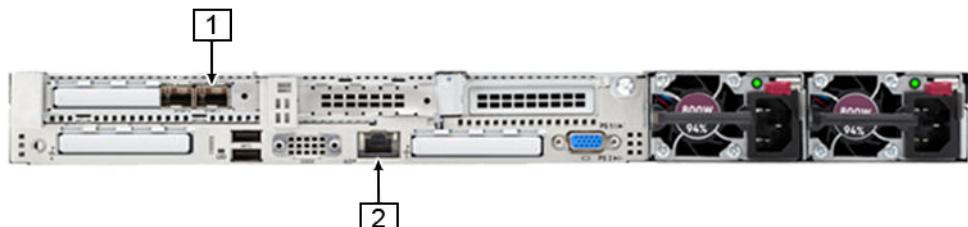
5. Verify that the Server is connected to a PDU (either data center PDU or rack mount) and/or connected to a UPS (either data center UPS or rack mount).

- If rack mount UPS is installed, verify that UPS is powered on, and that the KVM, Network switch and server are connected to UPS and PDU as shown below.



7.

- HPE ProLiant DL360 Gen10 Server High Tier: Verify that the High Tier server is connected to the network with one cable set on port (1) of the additional Ethernet controller and one cable set on the iLO port (2).



- HPE ProLiant DL360 Gen10 Server Low Tier: Verify that the Low Tier server is connected to the network with one cable set on port (1) of the Ethernet controller and one cable set on the iLO port (2).



- Verify that the KVM (or monitor) is connected to the VGA output and that the keyboard and mouse inputs are connected to the USB port(s).
- Verify that the UPS auto-shutdown USB input is connected to the one of the USB ports of the server.
- Apply power to the system. Apply power to the mains inputs of PDU and UPS (if applicable).
  - The UPS utility green LED should blink. The KVM turns on.
  - The Server on/off button LED should be steady yellow.
- Power up the UPS (if applicable) by pressing on the **On** button.

- The Network switch option turns on.
- The UPS Utility LEDs should display steady green as shown.

**Figure 2-3 HPE R/T3000 UPS front panel**



12. Power up the server by pressing on the **Power On** button.



- The Server power on/off button light turns from yellow to green.
  - There will be LED activity on the Server HDDs / SSDs and the LEDs shall be green.
  - The Network 1 LED should be ON (if the network is configured).
  - Hardware initialization sequence takes several minutes to complete. Please be patient. Then after a while, the screen unblanks and will display the HP ProLiant logo and boot up messages.
13. Verify that the following parameters are setup correctly, referring to the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware):
    - a. BIOS parameters (press **<F9>** to enter BIOS setup).

**NOTE**

The BIOS parameters can be checked at any time, without having to reboot the system and enter the BIOS menu as follow:

- In a terminal, login as **root**.
- Type the following command: **/sbin/conrep -s <Enter>**.
- The BIOS parameters are save locally in the file **conrep.dat**, and can be viewed using the command **cat conrep.dat <Enter>** or the command **more conrep.dat <Enter>**.

- b. iLO Service Processor parameters (press **<F8>** to enter iLO setup).
- c. RAID controllers / RAID levels parameters (press **<F8>** to enter RAID setup).
  - P440ar RAID controllers / RAID levels parameters

- 2 x 300GB HDDs in RAID 1
  - 6 x 600GB HDDs (Low Tier) in RAID 6 OR
  - 6 x 1.8TB HDDs (High Tier) in RAID 6
14. Quit the BIOS setup.

Once initialization is complete, the boot sequence will restart and complete as the AW Server has been preloaded by Manufacturing.

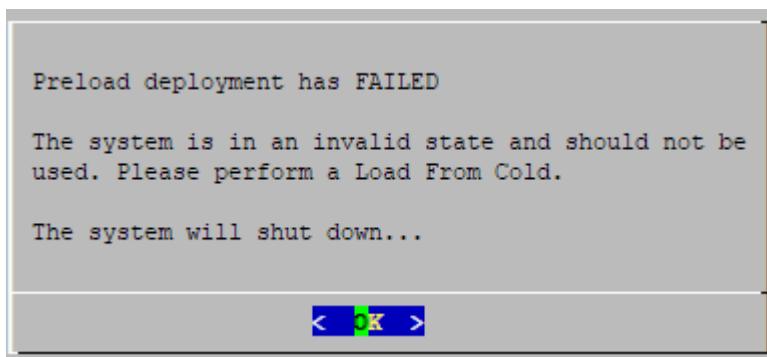
**NOTE**

When booting the AW Server, Scientific Linux progress bar is displayed for OS boot. However, details of other operations are not provided. To display the details, hit any of the arrow keys or the <Esc> key. This will display of OS boot messages including filesystem check progress. Hitting any of the arrow keys or the <Esc> key again displays the previous OS boot screen progress bar.

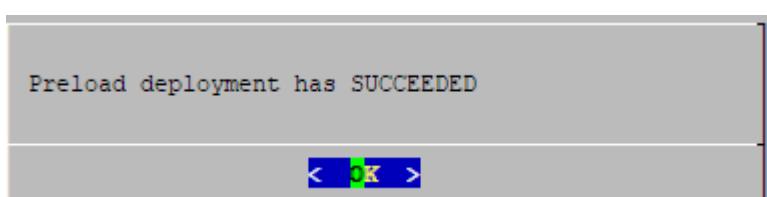
## 2.5.4 Finalizing Installation Verification

Obtain all necessary network configuration and time zone and region information from the site IT Admin.

1. When boot sequence has completed, login as **root**.
2. If the preload deployment failed, the following window appears:



- a. Press <Enter> to close the window.
- b. Proceed to a Load From Cold as described in [3.10 Job Card UPG001 - Software Upgrade on page 495](#).
3. If the preload deployment succeeded, the following window appears:



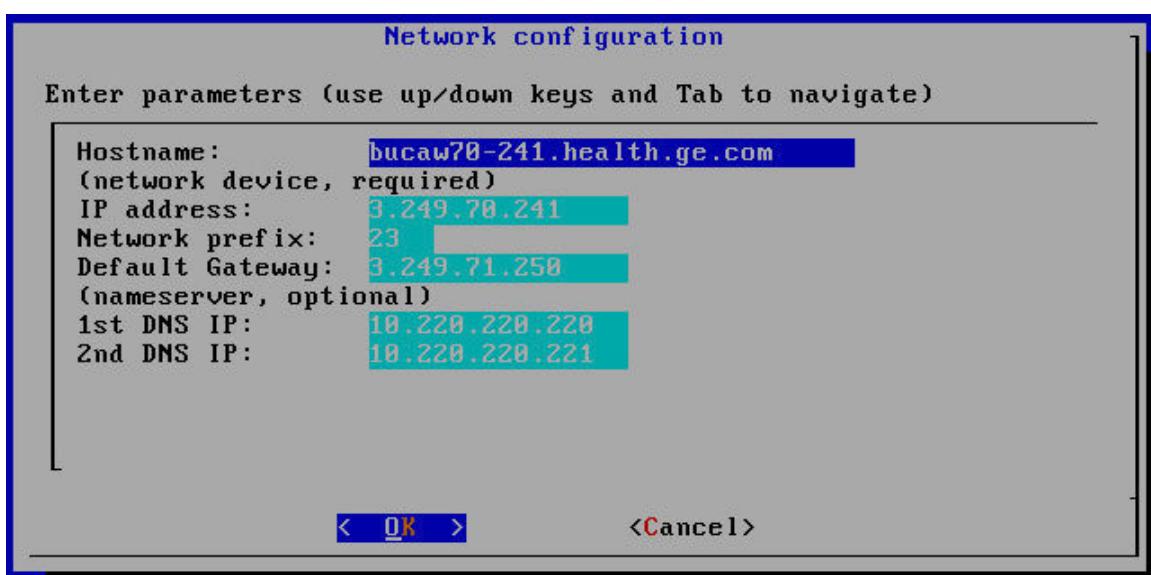
Press <Enter> to continue with the installation.

4. In the *Network configuration* window, keep <Setup> selected and press <Enter>

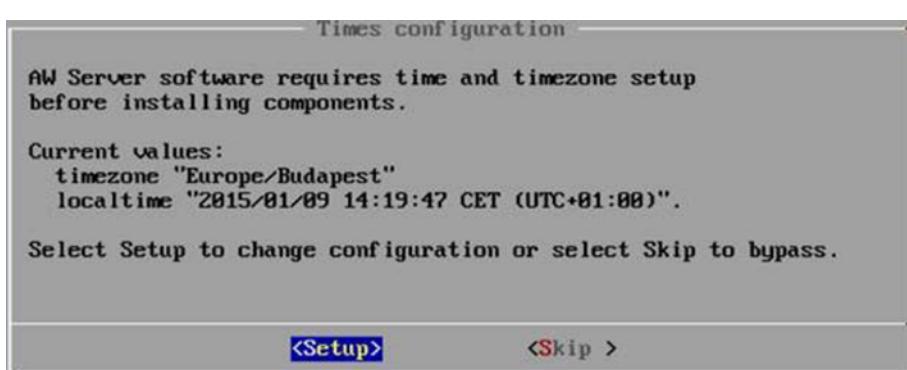


5. In the screen that appears, enter the network information:

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.



- Enter the Hostname (followed by "dot" Domain\_name if applicable).  
I.e: **aws-DL560.euro.health.ge.com**
  - Press arrow down to the **IP address**, **Network prefix** and **Default Gateway** fields to enter the parameters.
  - If applicable, enter the parameters for the DNS server(s).
  - Tab down to select <OK> and press <Enter> to save the configuration.
6. In the *Times configuration* window, keep <Setup> selected and press <Enter>.



7. In the screen that appears, enter the date and time information:

- a. Type the number corresponding to the region where the AW Server is installed, and press **<Enter>**.

```
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.
#? 2
Select a country (.. to skip back)
```

For instance, after selecting **2** for Americas the following screen appears:

```
1) ..          19) Dominica          37) Paraguay
2) Anguilla    20) Dominican Republic 38) Peru
3) Antigua & Barbuda 21) Ecuador          39) Puerto Rico
4) Argentina   22) El Salvador        40) St Barthelemy
5) Aruba       23) French Guiana     41) St Kitts & Nevis
6) Bahamas    24) Greenland         42) St Lucia
7) Barbados   25) Grenada          43) St Maarten (Dutch part)
8) Belize      26) Guadeloupe        44) St Martin (French part)
9) Bolivia     27) Guatemala         45) St Pierre & Miquelon
10) Brazil     28) Guyana           46) St Vincent
11) Canada     29) Haiti             47) Suriname
12) Caribbean Netherlands 30) Honduras         48) Trinidad & Tobago
13) Cayman Islands 31) Jamaica          49) Turks & Caicos Is
14) Chile       32) Martinique        50) United States
15) Colombia   33) Mexico            51) Uruguay
16) Costa Rica 34) Montserrat       52) Venezuela
17) Cuba        35) Nicaragua         53) Virgin Islands (UK)
18) Curacao    36) Panama           54) Virgin Islands (US)
#? █
```

- b. Type the number corresponding to the country where the AW Server will be installed, and press **<Enter>**:

For instance, after selecting **50** for US the following screen appears:

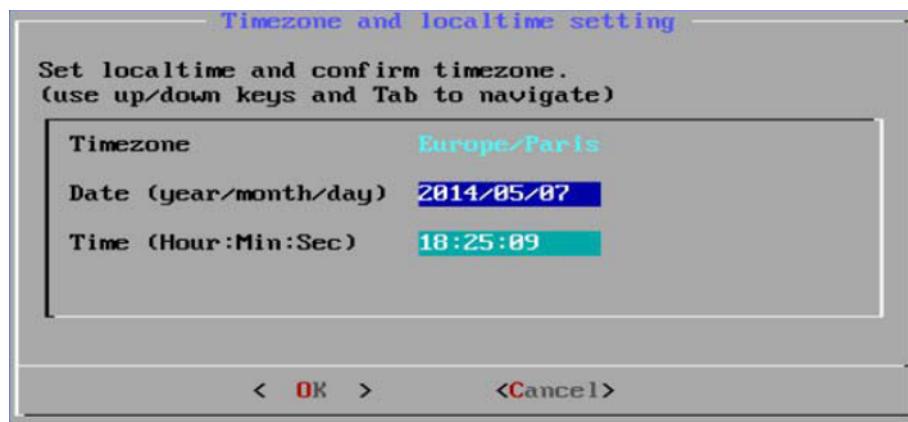
```
Select one of the following time zone regions (.. to skip back)
1) ..
2) Eastern Time
3) Eastern Time - Michigan - most locations
4) Eastern Time - Kentucky - Louisville area
5) Eastern Time - Kentucky - Wayne County
6) Eastern Time - Indiana - most locations
7) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
8) Eastern Time - Indiana - Pulaski County
9) Eastern Time - Indiana - Crawford County
10) Eastern Time - Indiana - Pike County
11) Eastern Time - Indiana - Switzerland County
12) Central Time
13) Central Time - Indiana - Perry County
14) Central Time - Indiana - Starke County
15) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
16) Central Time - North Dakota - Oliver County
17) Central Time - North Dakota - Morton County (except Mandan area)
18) Central Time - North Dakota - Mercer County
19) Mountain Time
20) Mountain Time - south Idaho & east Oregon
21) Mountain Standard Time - Arizona (except Navajo)
22) Pacific Time
23) Pacific Standard Time - Annette Island, Alaska
24) Alaska Time
25) Alaska Time - Alaska panhandle
26) Alaska Time - southeast Alaska panhandle
27) Alaska Time - Alaska panhandle neck
28) Alaska Time - west Alaska
29) Aleutian Islands
30) Hawaii
#? █
```

- c. Type the number corresponding to the Time zone region where the AW Server is installed, and press <Enter>.

**NOTE**

This step is required for countries having several Time zones.

The *Timezone and localtime setting* window appears:



- d. Modify the Date and Time if necessary.

Press <Down arrow> to check or modify the time accordingly.

- e. Tab down to select <OK> and press <Enter> to save the configuration.
8. In the *EA3 password change* window, press <Enter> to change passwords for the **admin** and **service** users.



A prompt asks to type the new password for the **admin** user.



9. Refer to [2.21 Job Card IST006 - Changing the Passwords on page 249](#) for the password change guidelines.

- Enter the new **admin** user password and press <Enter> to continue.

A prompt asks to type again the new password for the **admin** user.

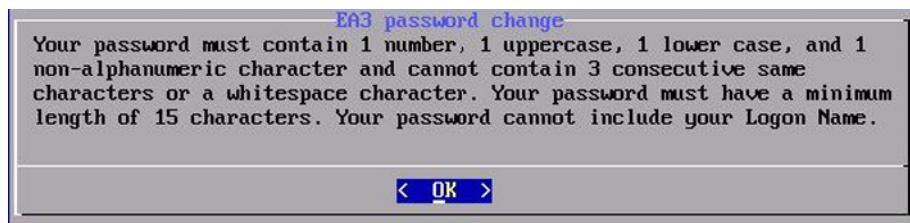


- Enter again the new **admin** user password and press **<Enter>** to confirm.

If the password is successfully updated, a notification appears.



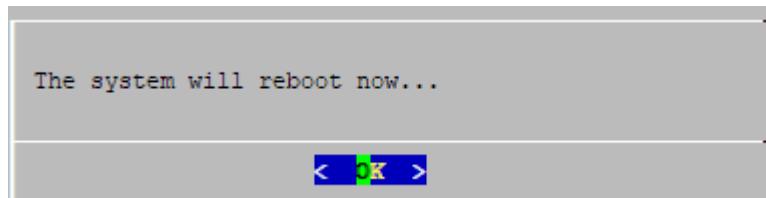
If the password does not comply with the password policy, enter a new password referring to the rules that appear.



- Repeat the procedure (from [Step 9](#) to [Step 10](#)) for the **service** user.

- Press **<Enter>**.

The following window appears.



- Press **<Enter>** to reboot.

- When boot sequence has completed, login as **root**.

- Verify that the OS sees the correct CPUs are installed with the following command levels, and corresponding results:

Command	Result
<code>cat /proc/cpuinfo   more &lt;Enter&gt;</code>	Complete information
<code>cat /proc/cpuinfo   grep -i processor &lt;Enter&gt;</code>	Filtered on ordered Processor numbers
<code>cat /proc/cpuinfo   grep -i CPU &lt;Enter&gt;</code>	Filtered on CPU info

There are 32 (2 x Sixteen-core) processors with a model name of "Intel(R) Xeon(R) CPU".

- Verify that the OS sees the correct amount of memory with the following command:

```
cat /proc/meminfo | grep -i memtotal <Enter>
```

26440444 kB (256GB) total memory.

- Verify the partitioning after the AWS load with the following command: `df -k <Enter>`.

#### NOTE

Alternatively, use the `df -h` command for a display in GBytes.

#### NOTE

System filesystem defaults to `sda`, backup and image filesystems to `sdb`.

**NOTE**

The Used and Available values may differ from those displayed in the examples below.

The example below is for a HP High Tier server.

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/sda3	51475068	10732160	38121468	22%	/
tmpfs	132202220	0	132202220	0%	/dev/shm
/dev/sda1	10190136	182172	9483676	2%	/var/log
/dev/sdb1	3778616	7932	3575408	1%	/export/backup
/dev/sdb2	5763456840	21092744	5449590672	1%	/export/home1

The example below is for a HP Low Tier server.

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/sda3	51475068	13244060	35609568	28%	/
tmpfs	32922124	0	32922124	0%	/dev/shm
/dev/sda1	10190136	187140	9478788	2%	/var/log
/dev/sdb1	3778360	7820	3575276	1%	/export/backup
/dev/sdb2	1726522184	21899712	1617713532	2%	/export/home1

18. Check the OS version, with the following command and results:

**cat /etc/aweos <Enter>**

```
OS: AWS3.2_OS_7.<x>, <x> depends on the OS version.
OS Build ID: yyyyymmdd I.e: 20190626
```

19. Check the AWS Platform version, with the following command and results:

**cat /etc/aweconfig <Enter>**

For AWS3.2 Ext.2.0 release:

```
AWE_HOME=/usr/share/awe
AWE_VERSION=aws-3.2-2.0-1728.2
AWE_BUILDDID=aws-3.2-2.0-1728.2
AWE_BUILDDATE=20170713
AWE_UDI='(01)00840682102384(10)AWS3D2E002D0'
AWE_REF='5719780'
AWE_LOT='AWS3D2E002D0'
AWE_USER=sdc
AWE_GROUP=sdc
HTDOCS=/var/www/html
APACHE_CONFDIR=/etc/httpd
AWE_JVMARGS="-Xmx1000m -Xss128k -server -Dtap.dm.ImageMemory=200
-XX:+UseParallelGC -XX:+AggressiveHeap"
```

**NOTE**

This is an example result. The actual values may differ at time of release of the software.

## 2.5.5 iLO Service Processor Firmware upgrade

Follow the below step to fix potential critical bugs and vulnerabilities with the iLO Service Processor Firmware:

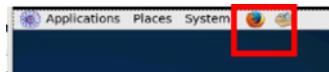
1. Open an Internet Navigator and login into the iLO Service processor ([http://<iLO\\_IP\\_address>](http://<iLO_IP_address>)) as **root**.

- In case you are in front of the server (in the datacenter):

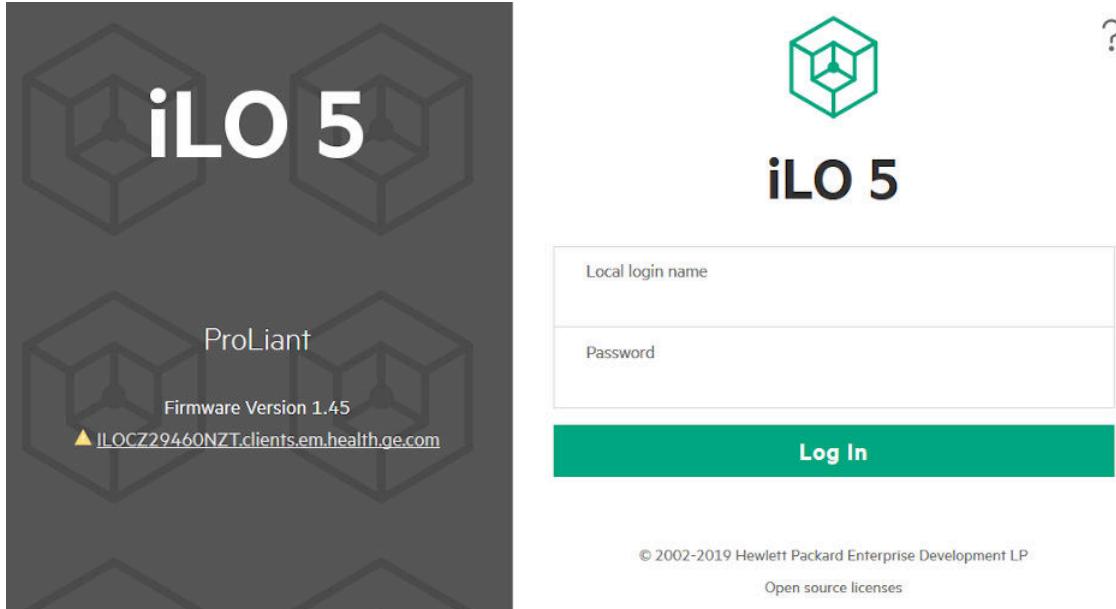
At the KVM, launch the graphical mode:

```
startx <Enter>
```

Open an Internet Navigator by clicking on the Firefox icon.



- In case you can access the server remotely, open the Internet Navigator on the Client PC or FE laptop.



- In **Information**, select the **Overview** tab.

Server		iLO	
Product Name	ProLiant DL360 Gen10	IP Address	10.120.58.165
Server Name	awsbuc20ltg5	Link-Local IPv6 Address	FE80::9640:C9FF:FE32:E1B6
Operating System	SLES 15.4	iLO Hostname	ribfbucaws20ltg5
System ROM	U32 v2.30 (02/11/2020)	iLO Dedicated Network Port	Enabled
System ROM Date	02/11/2020	iLO Shared Network Port	Disabled
Redundant System ROM	U32 v2.30 (02/11/2020)	iLO Virtual NIC	16.1.15.1
Server Serial Number	CZ201304M7	License Type	iLO Advanced
Product ID	P19766-B21	iLO Firmware Version	2.12 Jan 17 2020
UUID	37393150-3636-5A43-3230-313330344D37	iLO Date/Time	Thu Feb 20 09:05:02 2020
<a href="#">Remote Console</a>		<a href="#">HTML5</a>	<a href="#">Java Web Start</a>

Note the version and date of the iLO firmware.

- From the Client PC or FE laptop, connect to HPE support website at:

[https://support.hpe.com/connect/s/product?  
language=en\\_US&kmpmoid=1010145741&tab=manualsAndGuides](https://support.hpe.com/connect/s/product?language=en_US&kmpmoid=1010145741&tab=manualsAndGuides)

- In the **Drivers and Software** tab, click on **Firmware** and filter on the **Subtype** and **Operating Environment Type**, as shown in the image below, to view the latest patches available.

Severity	Type   Subtype	Title	Version	Environment
●	Firmware   Lights-Out Management	<a href="#">Online ROM Flash Component for Windows x64 - HPE Integrated Lights-Out 5</a>	2.91 2023-05-24	
●	Firmware   Lights-Out Management	<a href="#">Online Flash Component for Windows x64 - HPE Integrated Lights-Out 5 Chinese Simplified Language Pack</a>	2.72 2022-11-01	
●	Firmware   Lights-Out Management	<a href="#">Online Flash Component for Windows x64 - HPE Integrated Lights-Out 5 Japanese Language Pack</a>	2.72 2022-10-05	

#### NOTE

In the image above the patches may be different as this image is only for reference to help navigating in this procedure.

#### NOTE

Check for critical patch (a patch is critical if in the Severity column the icon is displayed). In this example there is no critical patch.

If there is no critical patch or if the patch is already installed (it is the same as the iLO firmware version shown in Step 2), skip this section. Otherwise continue with the next steps.

- Select the critical patch, in the page that displays click on **Download software** and then on **Download** in the popup that displays.
- Verify the checksum of the downloaded file:

For instance:

```
certutil -hashfile cp057117.exe SHA256 <Enter>
```

- Double-click the downloaded file, and then click the **Extract** button. Select a location for the extracted files, and then click **OK**.

#### NOTE

The name of the iLO firmware image file (BIN file) is similar to `ilo5_<yyy>.bin`, where `<yyy>` represents the firmware version (for instance `ilo5_291.bin`).

- In case you are in front of the server (in the datacenter):
  - From the PC/laptop copy the BIN file into an USB media.
  - Insert the USB media into an USB port of the server.
  - Acknowledge the warning message that pops up.

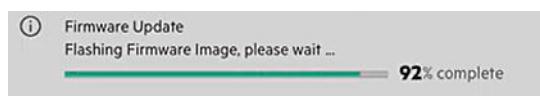
A shortcut with the content of the USB media appears. Double-click on it to display the path of the BIN file.

- In the iLO Service processor, select **Firmware & OS Software**. Then on the right part select **Update Firmware**.

Firmware Name	Firmware Version	Location
iLO 5	2.12 Jan 17 2020	System Board
System ROM	U32 v2.30 (02/11/2020)	System Board
Intelligent Platform Abstraction Data	11.0.0 Build 15	System Board
System Programmable Logic Device	0x31	System Board
Power Management Controller Firmware	1.0.7	System Board
Power Supply Firmware	1.04	Bay 1
Power Supply Firmware	1.04	Bay 2
Innovation Engine (IE) Firmware	0.2.1.2	System Board
Server Platform Services (SPS) Firmware	4.1.4.339	System Board
Smart Storage Energy Pack	0.70	Energy Pack 1
Redundant System ROM	U32 v2.30 (02/11/2020)	System Board

- In the **Flash Firmware** panel, click on **Choose File**, point to the BIN file and select it.

- Click on **Flash** button and acknowledge the warning message that pops up.
- Wait for the update process to complete.



After a successful update, the iLO will automatically restart, the server will not be affected, it will work continuously.

13. Login again into the iLO Service processor. In **Information**, select the **Overview** tab and check the version and date of the iLO firmware.

Server		iLO	
Product Name	Proliant DL360 Gen10	IP Address	10.120.58.165
Server Name	awsbuc20ltg5	Link-Local IPv6 Address	FE80::9640:C9FF:FE32:E1B6
Operating System	SLES 15.4	iLO Hostname	ribfrbucaws20ltg5
System ROM	U32 v2.30 (02/11/2020)	iLO Dedicated Network Port	Enabled
System ROM Date	02/11/2020	iLO Shared Network Port	Disabled
Redundant System ROM	U32 v2.30 (02/11/2020)	iLO Virtual NIC	16.1.15.1
Server Serial Number	CZ201304M7	License Type	iLO Advanced
Product ID	P19766-B21	iLO Firmware Version	2.91 May 18 2023
UUID	37393150-3636-5A43-3230-313330344D37	iLO Date/Time	Fri Jun 16 09:05:02 2023
<a href="#">Remote Console</a> <a href="#">HTML5</a> <a href="#">.NET</a> <a href="#">Java Web Start</a>			

14. In case you are in front of the server (in the datacenter), eject and remove the USB media from the USB port of the server.

## 2.6 Job Card IST001AB - Hypervisor Configuration

### 2.6.1 Overview

This section applies to the Hypervisor configuration on a customer's physical server.

It allows installing and configuring the Hypervisor environment for the creation and the management of the virtual machine(s) hosting the virtual AW Server.

**All sections are performed and completed by the IT Administrator of the site.**

Make sure the physical server has the required characteristics and the minimal resources to support the Virtual AW Server installation, defined in the **Pre-Installation Manual** and summarized below:

#### Physical server (host) characteristics:

- Intel Xeon CPUs supporting SSE 4.1 and AES instructions
- 1 Ethernet device (minimum 1Gb/s)
- Data store to store all VM data with thick provisioning, including provision for Windows and VM swap files (210GB).
- Data store to store images (300GB min - 6TB max)
- Enough RAM to satisfy virtual RAM requirements without RAM over commit

#### NOTE

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

#### Virtual Machine (hosted) characteristics:

AWS Low Tier	AWS High Tier	HAPS server
processor: 8 vCPUs	processor: 24 vCPUs	processor: 2 vCPUs
disk: one 210GB vHDD	disk: one 210GB vHDD	disk: one 210GB vHDD
memory: 24/64/96GB*	memory: 64/72/104GB*	memory: 4GB
network: 1 x Ethernet	network: 1 x Ethernet	network: 1 x Ethernet

\*RAM depends on integration mode, see table in Section [2.4.1 Virtual AW Server Characteristics on page 36](#)

#### NOTE

As the host, the Virtual Machine shall support the SSE 4.1 instructions. If it is not the case, it could lead to Applications start failure.

If not, you shall configure the hypervisor EVC mode to a level which supports SSE 4.1 instruction.

As the host, the Virtual Machine shall support the AES instructions.

#### Hypervisor configuration process summary:

1. The IT admin installs, configures and connects to the Hypervisor.

#### NOTE

Installation and Configuration of the Hypervisor environment for Virtual AW Server is under the Customer's responsibility.

For **VMware** hypervisor (ESXi) refer to the corresponding documentation.

For **Microsoft** hypervisor (Hyper-V) refer to the corresponding documentation.

2. The IT admin allocates the physical network port(s) of the Hypervisor necessary for the virtual AW Server. - [2.6.2 Ethernet ports Allocation on page 60](#)
3. The IT admin creates a "service" account so that the GE FE will be able to administrate the virtual AW Server. - [2.6.3 Create a GEHC service user account on page 63](#)
4. The IT admin makes sure a NTP server is setup for the Hypervisor - See [2.6.4 Setup a NTP server for the Hypervisor on page 67](#)

#### NOTE

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

## 2.6.2 Ethernet ports Allocation

### 2.6.2.1 Foreword

#### Requirement on physical network card

The minimum requirement to install a virtual AW Server is to have one physical network card dedicated to the AW Server VM. This requirement applies to each hypervisor that will host the virtual AW Server.

The Virtual machine containing the virtual AW Server will have 1 virtual network card. This is defined in the settings of the OVF Template.

#### Requirement on port groups and virtual switch

For the virtual network card of the VM, the minimum requirement is to have one port group connected to one 1GB/s physical network card. The port group contains only the AW Server Virtual Machine. This way the physical network card is dedicated to the virtual AW Server.

It is also possible to have other Virtual Machines using the same port group. However in this case, it is needed to have the same number of physical network card and of Virtual Machines in the virtual switch.

### Resource preparation for Virtual Machine

It is important to check that enough resources are available for the AW Server Virtual Machine:

- CPU (no hyperthreading)
- Memory
- Storage

Also, if several AW Server Virtual Machines are going to be installed, the minimum requirements have to be multiplied by the number of VM.

Also keep in mind that CPU and RAM should not be over committed for the AW Server. The AW Server VMs always need access to the resources described in minimum requirements.

## 2.6.2.2 Procedure

### NOTE

The steps below are provided as an example to configure the network on one single hypervisor with 4 physical network cards that will host one virtual AW Server. For details on the network configuration for more advanced configuration and clusters, refer to the related documentation.

The following example is based on the use of a physical server equipped with a Network controller fitted with 4 Ethernet ports. In our example, the physical server will be used to host Virtual machine(s) (virtual AW Server(s)).

Using bigger physical servers with higher capacity and a greater number of Ethernet controllers and/ or Ethernet ports allows hosting of a higher number of virtual machines, however the settings of these servers follow the same philosophy.

**Always make sure that the Virtual AW Servers will have the necessary bandwidth.**

### Necessary Networking Hardware resources:

The virtual AW Server needs one 1GB/s physical network card (Ethernet port) dedicated only to the AW Server.

The 1 GB/s physical network card is dedicated to communication with the other hosts and to communication between the nodes of the cluster, on the Hospital network .

### NOTE

It is recommended to use a separate NIC for the Management network of the Hypervisor, in order to ensure that enough bandwidth will be available during template deployment or other similar operations.

Below are the instructions to configure vSphere networking for virtual AW Server(s).

1. Login to the vSphere Web Client:

- a. Enter the URL for the vSphere Web Client in your web browser:  
`https://<client-hostname>/vsphere-client`
- b. Select **LAUNCH VSPHERE WEB CLIENT (FLEX)**.
- c. Enter the **administrator** login and password. Check with the IT admin for the login/ password.

2. In the *vSphere Web Client* page that displays:

Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP ranges
Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet					
vmnic0	1000 Mb	Auto negotiate	vSwitch0	28:80:23:a5:53:34	3.213.70.1-3.213.70.31...
vmnic1	Down	Auto negotiate	--	28:80:23:a5:53:35	No networks
vmnic2	1000 Mb	Auto negotiate	vSwitch1	28:80:23:a5:53:36	3.213.70.1-3.213.70.31...
vmnic3	Down	Auto negotiate	--	28:80:23:a5:53:37	No networks
vmnic4	1000 Mb	Auto negotiate	vSwitch0	28:80:23:9b:44:74	3.213.70.1-3.213.70.31...
vmnic5	Down	Auto negotiate	--	28:80:23:9b:44:75	No networks

- a. Select the Hypervisor and click on **Configure**.
- b. Expand **Networking** sub-menu and click on **Physical adapters** to see the available Ethernet ports and their status.  
The *Physical adapters* panel displays. You can read information about the different adapters such as their speed and the virtual switch they are linked to.
- c. Check how many network cards are available and which one you plan to attribute to the Virtual machines that are going to be created.
3. Create a virtual switch for the virtual AW Server:  
Virtual switches are entities used by vSphere to link virtual network card of a Virtual Machine to physical network card of the server hardware.
  - a. Click on the  icon.  
The *Add Networking* wizard displays.
  - b. Select the **Virtual Machine Port Group for a Standard Switch** radio button and click on **Next**.
  - c. In the panel that displays, select **New standard switch** radio button and click on **Next**.
  - d. In the panel that displays, click on the **+** icon.
  - e. In the sub-screen that displays, select the next available **Network Adapter** and click on **OK**.
  - f. Click on **Next**.
  - g. In the panel that displays, type in the **Network label** (AWS3 Hospital Network, for example) and click on **Next**.  
The *Ready to Complete* panel displays.
  - h. Click on **Finish**.
4. Follow the same procedure to setup other Network adapters if needed and create the vSphere standard switches that will be attributed to the Virtual machines (AW Servers) once they have been created.
5. Follow the same procedure to setup the Network adapter for the AW Server Private Network.

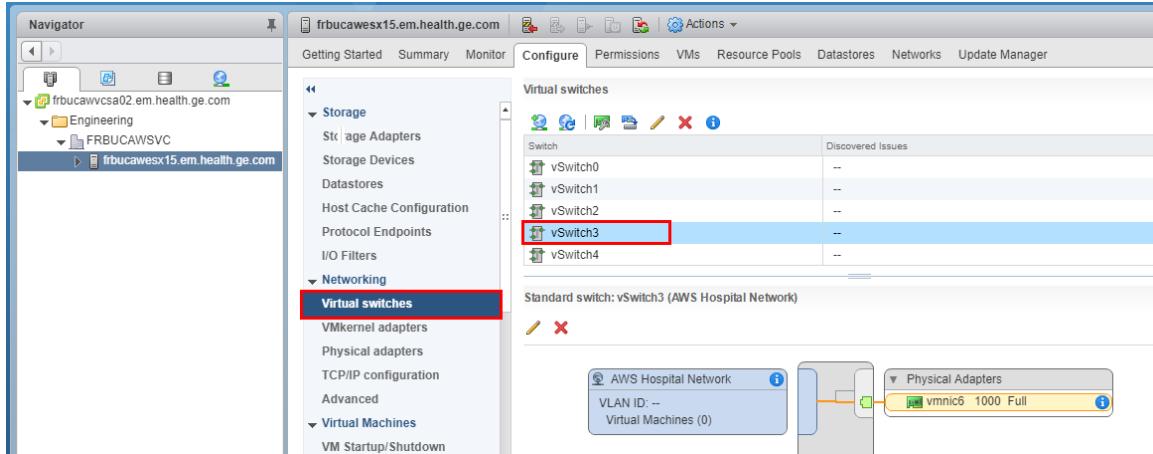
#### **NOTE**

Two or more virtual AW Servers hosted on the same physical server can share the same physical Network adapter for the AW Server Private Network.

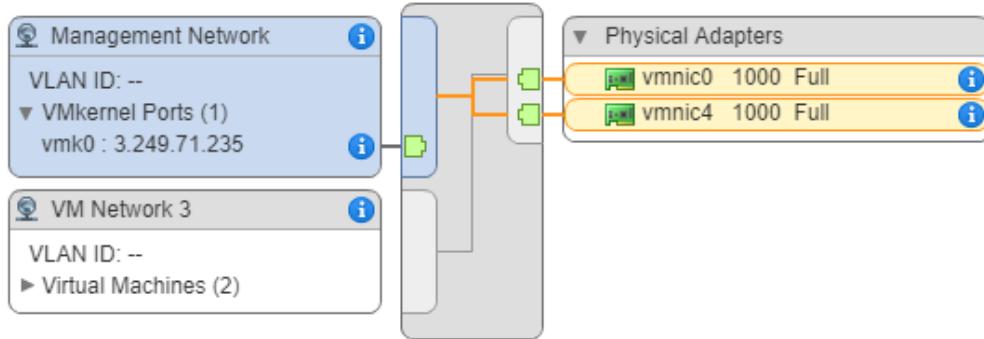
6. Display the configuration of the virtual switch by clicking on **Virtual switches** then on the switch previously created.

The *Standard switch* panel displays. This view displays the current configurations of the virtual switches for this Hypervisor.

- When complete, the configuration should display as follows:



- There is also a virtual switch that contains the *Management network*. This virtual switch is used to indicate what physical network card is used for communication between the Hypervisor and the vSphere clients.



It is recommended to keep a dedicated virtual switch for Management Network.

- Optional: if the *VM Network* displays as linked to the *Management Network*, as in the example above, you need to remove it:
  - Select the switch containing the *Management Network*.
  - Select the **Management Network** and click on the red cross in the *Standard switch* part of the panel.
  - Click on **Yes** to acknowledge the confirmation message that pops up.

This completes the Network ports allocation.

Proceed to [2.6.3 Create a GEHC service user account on page 63](#).

## 2.6.3 Create a GEHC service user account

In order to allow the GEHC FE to complete the installation of the virtual AW Server (virtual console access, virtual DVD drive usage...), it is needed to provide him/her an "hypervisor" account with the sufficient permissions on the AW Server Virtual Machine.

Below are the steps to configure a role and a local user on one single hypervisor. For more advanced configuration, refer to the related documentation.

- Connect to the ESXi Web Interface.

In a web browser enter the URL or IP address of the ESXi:

<https://<ESXi URL or IP>>

The *ESXi Web Interface* login screen displays.

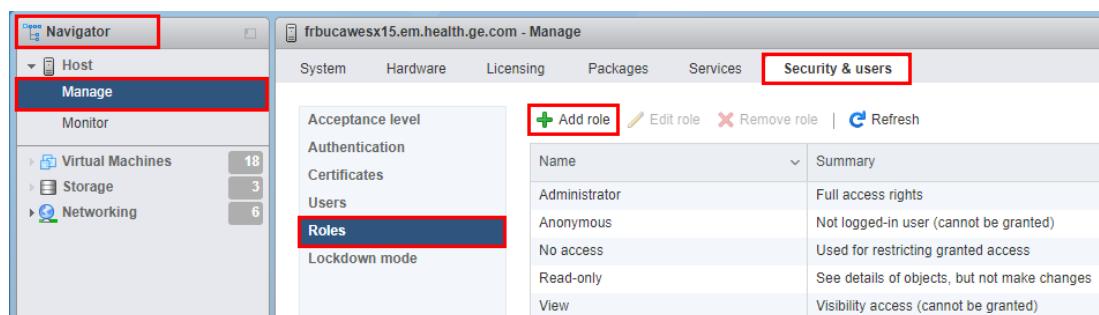
2. Enter the **root** login and password. Check with the IT admin for the password.

The *vSphere Web Client* page displays.

3. Create a GE Service role with appropriate permissions. As a first step, a new GE Service role shall be created with the necessary permissions to administrate a Virtual machine.

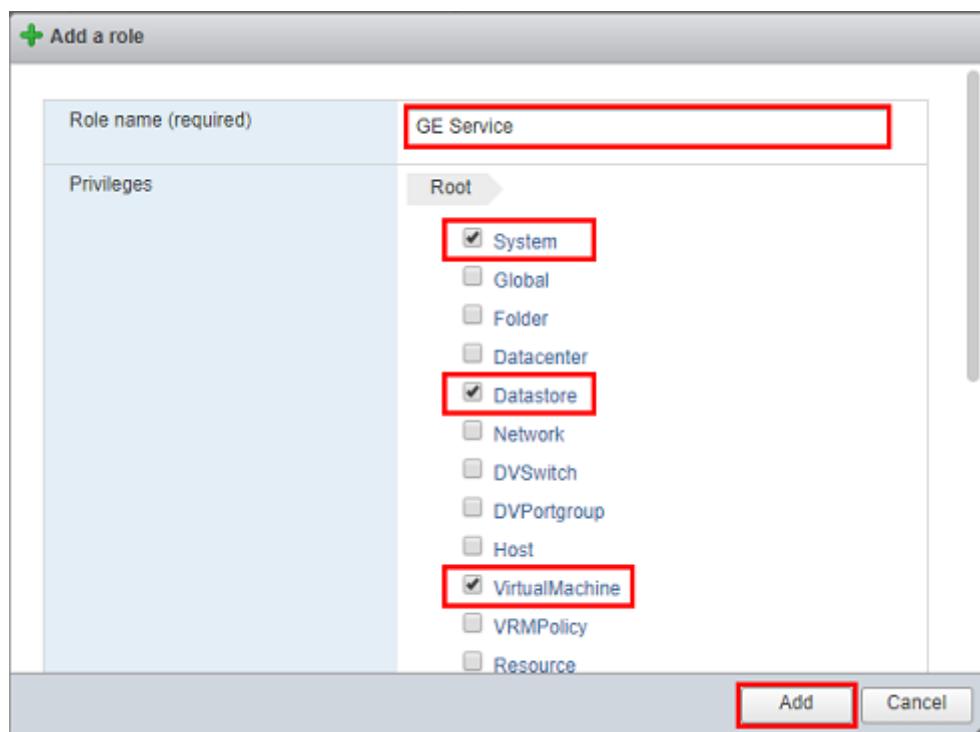
- a. In the *Navigator panel*, expand **Host** and click on **Manage**.

- b. Click on the *Security & Users* tab and select **Roles**.



- c. Click on the **Add role** icon.

The *Add a role* screen displays.



- d. Name the new role **GE Service**.

- e. Give the following permissions by checking the boxes:

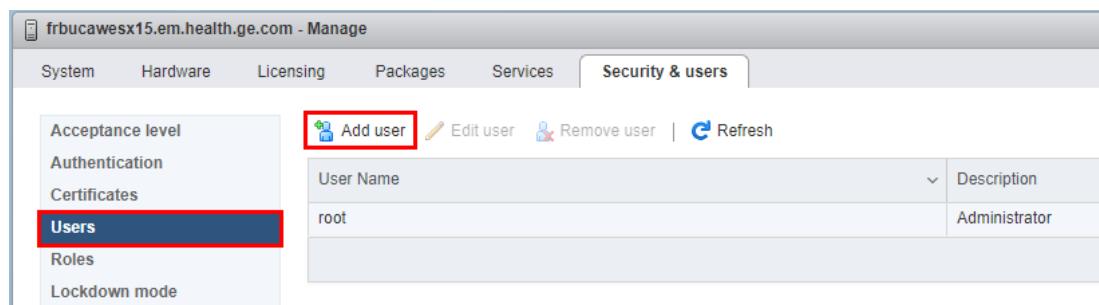
- **System**
- **Datastore**
- **Virtual machine**

- f. Click on **Add**.

The new **GE Service** role displays in the list of existing Roles.

4. Create a service user:

- In the **Security & Users** tab, select **Users**.



- Click on the **Add user** icon.

The *Add a user* screen displays.

User name (required)	service
Description	
Password (required)	.....
Confirm password (required)	.....
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

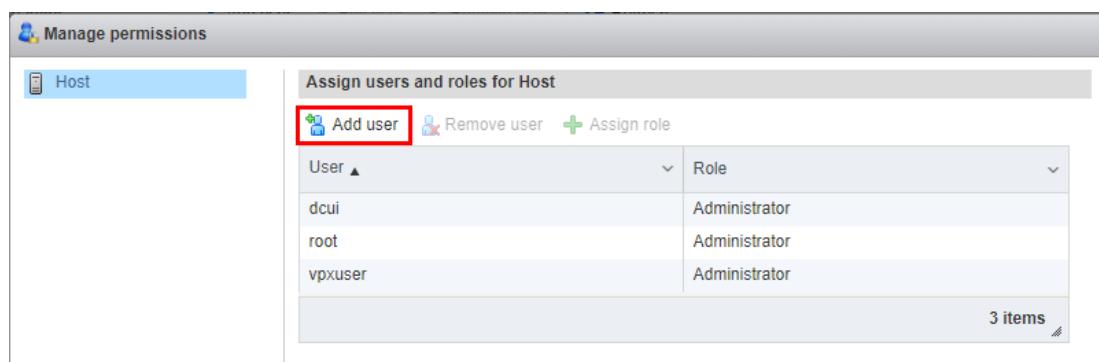
- Name the new user **service**.
- Type the password twice in the **Password** and **Confirm password** fields
- Click on **Add**.

A new user **service** displays in the list of Users.

5. Assign the GE Service role permissions to the service user:

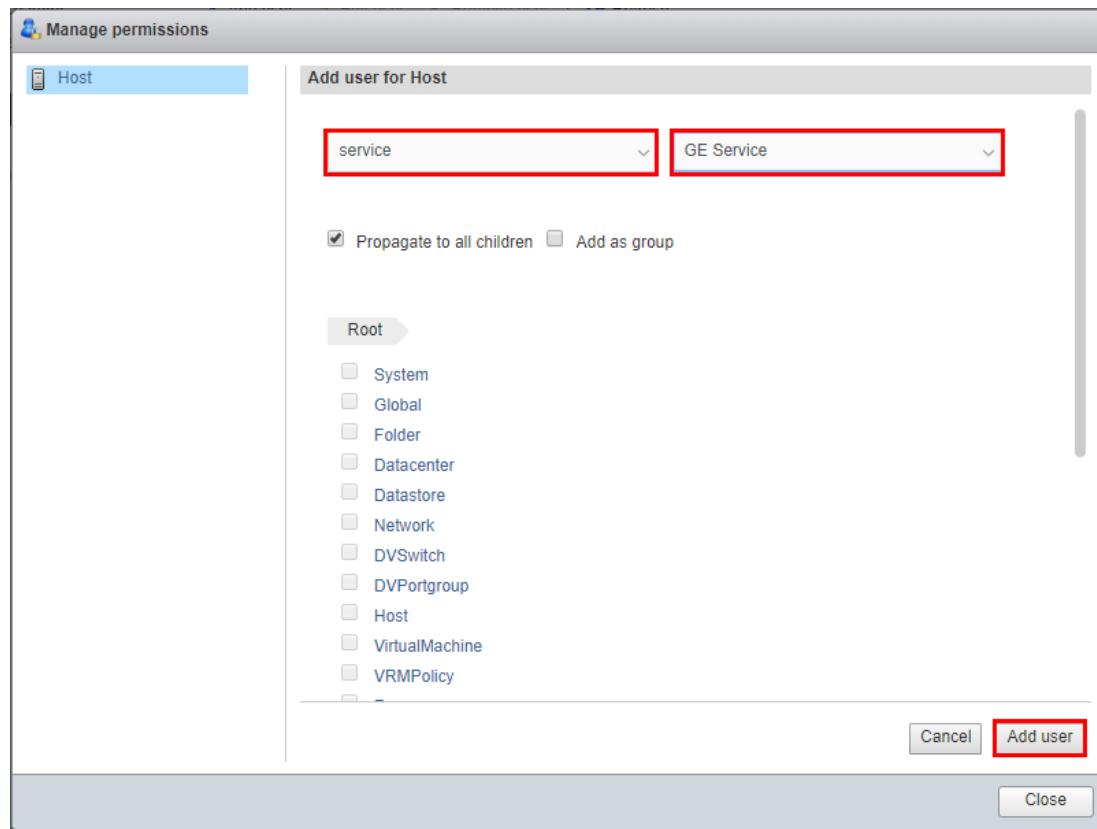
- In the *Navigator* panel, right click on **Manage** and select **Permissions**.

The *Manage permissions* wizard displays.

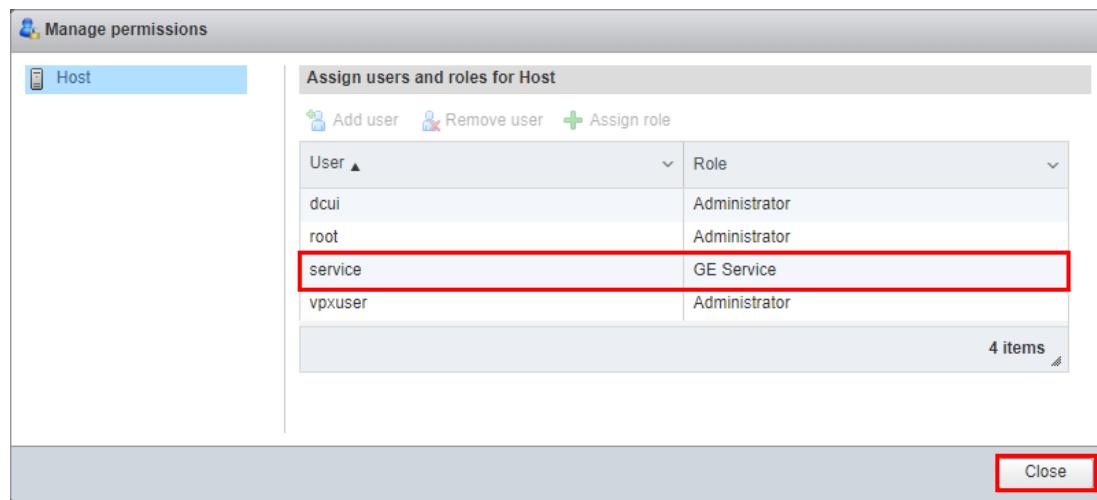


- b. Click on the **Add user** icon.

The *Add user for Host* panel displays.



- c. On the second drop-down menu, select the newly created **GE Service** role.  
d. Click on the **Add user** button.  
e. The user service displays in the list of users with the GE Service role.



- f. Click on **Close**.
- The service user gets linked to the GE Service role with the appropriate permissions.
6. Logout from ESXi Web Interface and login again with the service user credentials in order to check that the account is operational and addresses the virtual machine created to host the virtual AW Server:

**User: service**

**Password:** the password you specified in [Step 4.d.](#)

This completes the installation of the GE Service account.

Proceed to [2.6.4 Setup a NTP server for the Hypervisor on page 67.](#)

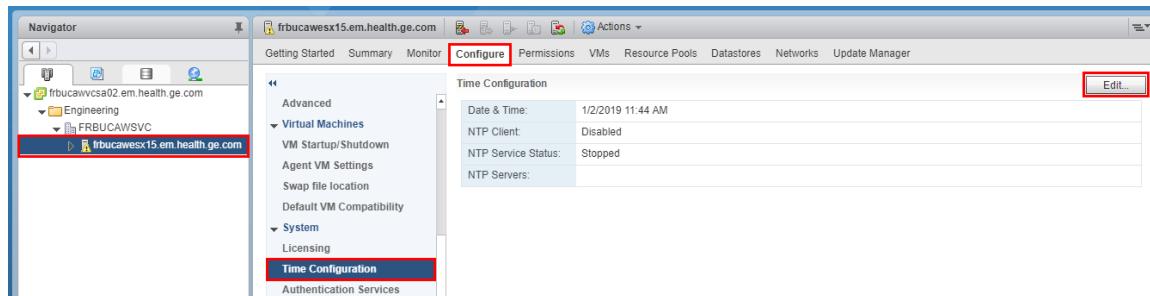
## 2.6.4 Setup a NTP server for the Hypervisor

It is recommended to configure a NTP server on each Hypervisor that will host the AWS Virtual Machine.

Below are the instructions to configure a NTP server on a single Hypervisor.

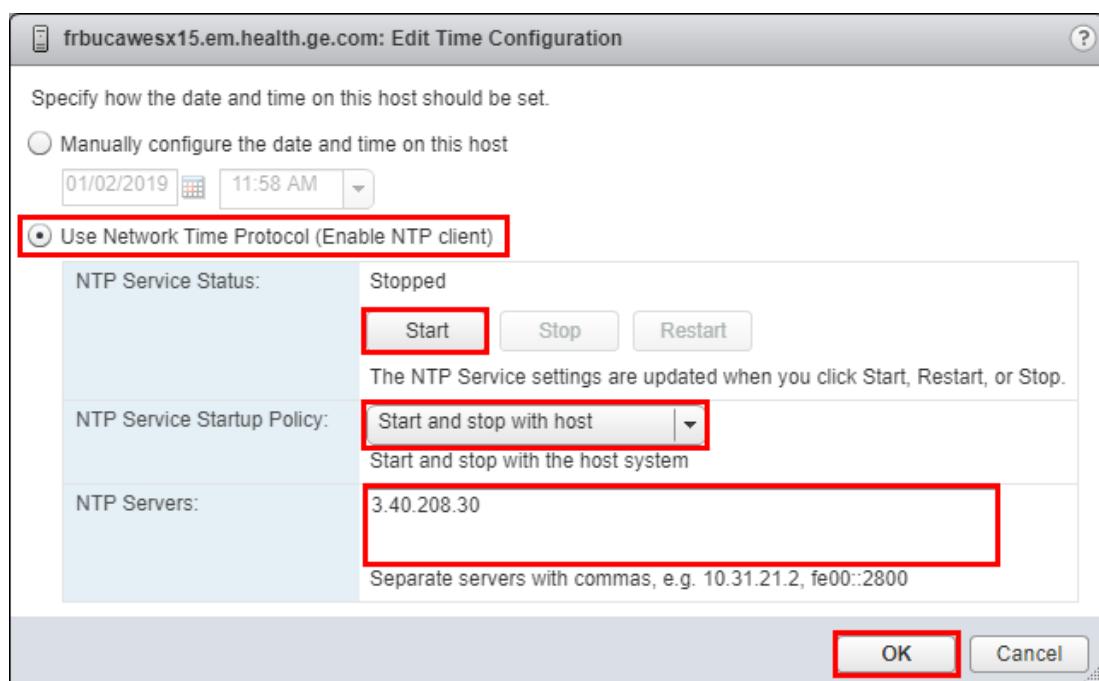
The correct time is essential to your Hypervisor, you will need it for a variety of reasons (syslog, iscsi authentication and Security) and your Virtual Clients.

1. Make sure you are logged on the vSphere Web Client as **administrator**.
2. In the main *vSphere Web Client* screen:



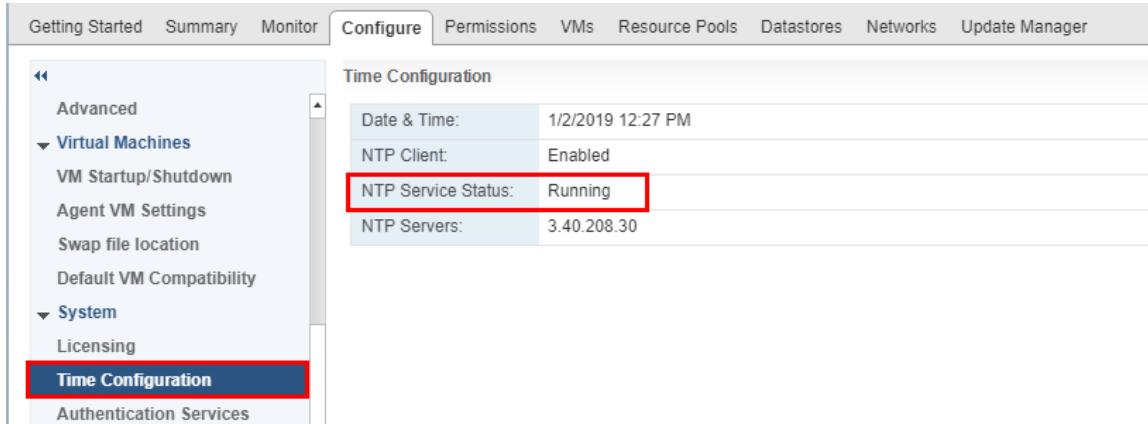
- a. Select the Hypervisor and click on the *Configure* tab.
  - b. Expand the **System** sub-menu and click on **Time Configuration**.
  - c. Click on the **Edit** button.
3. Configure and start the NTP server on the *Edit Time Configuration* screen:

- a. Select the **Use Network Time Protocol (Enable NTP client)** radio box.



- b. In the **NTP Servers** field, enter the site's NTP server name (I.e: ntp.pool.org) or NTP server's IP address.

- c. Set the **NTP Service Startup Policy** to **Start and stop with host**
  - d. Start the NTP service by clicking on the **Start** button.
  - e. Click on **OK** to complete the NTP server installation.
4. Verify that the NTP service has been started and is running.



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 Hypervisor.

This completes the Hospital IT Admin Hypervisor installation and configuration steps.

Proceed to [2.7 Job Card IST001B - Virtual Machine creation on page 68](#).

## 2.7 Job Card IST001B - Virtual Machine creation

### 2.7.1 Overview

#### NOTE

For the AW Server integrated within the CT/MR Console Environment (Edison HealthLink or CT Console), refer to [2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink on page 307](#) or [2.30 NanoCloud AW Server Installation in CT Console on page 373](#).

This section applies to the Virtual Machine creation on a customer's physical server.

**All sections are performed and completed by the IT Administrator of the site.**

#### Pre-requisite:

The Hypervisor is installed and configured. See section [2.6 Job Card IST001AB - Hypervisor Configuration on page 59](#).

#### Preliminary Steps:

1. The GEHC FE makes sure what type of Virtual AW Server has been purchased by the site and delivers the following information to the IT administrator of the site.
  - Low Tier or High Tier virtual AW Server (needs additional step to upgrade the default Low Tier VM to High Tier VM - See section [2.7.2.2 Steps to upgrade / downgrade a Virtual Machine on page 75](#)).
  - Integrated or Standalone (Non-Integrated) virtual AW Server (Standalone or Hybrid integration AW Server needs additional step to create hard disk for Image data - see section [2.7.2.3 Creating the image data disk for Standalone \(Non-Integrated\) and Hybrid AW Server on page 77](#))

- AW Server part of a cluster of virtual AW Servers (Scalability).

It is necessary to **also create two VMs** to host the HAPS (Preferences Sharing) servers.

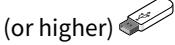
- See section [2.7.2.2 Steps to upgrade / downgrade a Virtual Machine on page 75](#) to downgrade the Low Tier VM to HAPS server VM
- Virtual servers in cluster mode need one dedicated physical network port (for hospital network communication and for AW Server communication between the AW Servers and HAPS). See [2.8 Job Card IST001C - Virtual Servers Cluster Installation Steps on page 80](#) for Scalability network setup.

2. The GEHC FE delivers the media necessary for VM creation, OS and AW Server installation to the IT administrator of the site.

### **Prepare the OVF Template software media that will be needed for installation:**

The software is delivered either:

- In the [Physical Software Kit on page 23](#). Use one of the following files, depending on the integration type:

Part Number	Content	Purpose	Integration Mode
5818084-10 	<i>aws-3.2-4.9-0.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) and the AWS software.	DDC
5872674-6 	<i>AWS3.2_OS_7.2-Scientific-7.9.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) only.	No-integ Hybrid Seamless

#### **NOTE**

The reference checksums files (.sha256 extension) are not listed in the table.  
However, they are present in the USB media to verify files integrity.

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use one of the following files, depending on the integration type, to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	Integration Mode
<i>5865566-5_AW_Server_3.2_Ext.4.9_and_OS_OVA_Template_for_VM.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) and the AWS software.	DDC
<i>5865564-5_AW_Server_3.2_Ext.4.9_OS_Only_OVA_template_for_VM.ova</i>	This OVA template is used for <b>Initial Installation</b> on VMWare <b>ESXi</b> environment. It allows to create a Virtual Machine with the OS (Scientific Linux 7.9) only.	No-integ Hybrid Seamless

#### **NOTE**

The reference checksums, to verify files integrity, are listed in the *packagemetadata.json* files.

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

**AW Server VM creation process summary:****NOTE**

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

1. The GE FE gives the site IT administrator, the OVF template software media that is needed for creating the Virtual machine, aimed to host the virtual AW Server.

The GE FE also delivers the following installation instructions to the site IT administrator. The OVF Template creates the Low Tier Virtual machine with the required characteristics to host the virtual AW Server, and loads the Linux OS alone or the Linux OS + the AW Server at the same time.

2. The IT admin connects to the Hypervisor.
3. The IT admin installs and configures the Hypervisor environment. See section [2.6 Job Card IST001AB - Hypervisor Configuration on page 59](#).
4. The IT admin loads the OVF template and creates the virtual machine (Low Tier) - Section [2.7.2.1 OVF Template Installation on page 71](#)
5. If the site has purchased a High Tier virtual AW Server, the GE FE notifies the IT admin that section [2.7.2.2 Steps to upgrade / downgrade a Virtual Machine on page 75](#) shall be performed, in order to upgrade the Low Tier VM into a High Tier VM.

If not, proceed to next step.

6. If the site has purchased a virtual AW Server cluster solution, the GE FE notifies the IT admin that, in addition to the AW Servers VMs, two HAPS server VMs shall be created from the Template, and that section [2.7.2.2 Steps to upgrade / downgrade a Virtual Machine on page 75](#) shall be performed, in order to downgrade the Low Tier VM into a HAPS server VM.
7. If the site has purchased a Standalone (Non-Integrated) virtual AW Server, the GE FE notifies the IT admin that section [2.7.2.3 Creating the image data disk for Standalone \(Non-Integrated\) and Hybrid AW Server on page 77](#) shall be performed, in order to create a virtual Hard disk to store the image data.

**NOTE**

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

## 2.7.2 Virtual machine creation

The IT Administrator of the site is responsible for installing, and configuring on-site a fully-functional Virtual machine with the appropriate characteristics for hosting the virtual AW Server. The IT Administrator of the site is also responsible for providing an "hypervisor" account for GE

service, so that the GEHC FE is able to administrate (load software, configure, etc..) the virtual machine which will host the virtual AW Server.

#### **Pre-requisite:**

Ask the IT administrator of the site for the network parameters necessary for your virtual AW Server and its environment.

- IP address of the Hypervisor.
- IP addresses and netmasks/network prefix to be used for the virtual AW Server.
- IP addresses used for the PACS.
- IP addresses used for the remote hosts (if applicable).
- IP addresses used for the printers (if applicable).

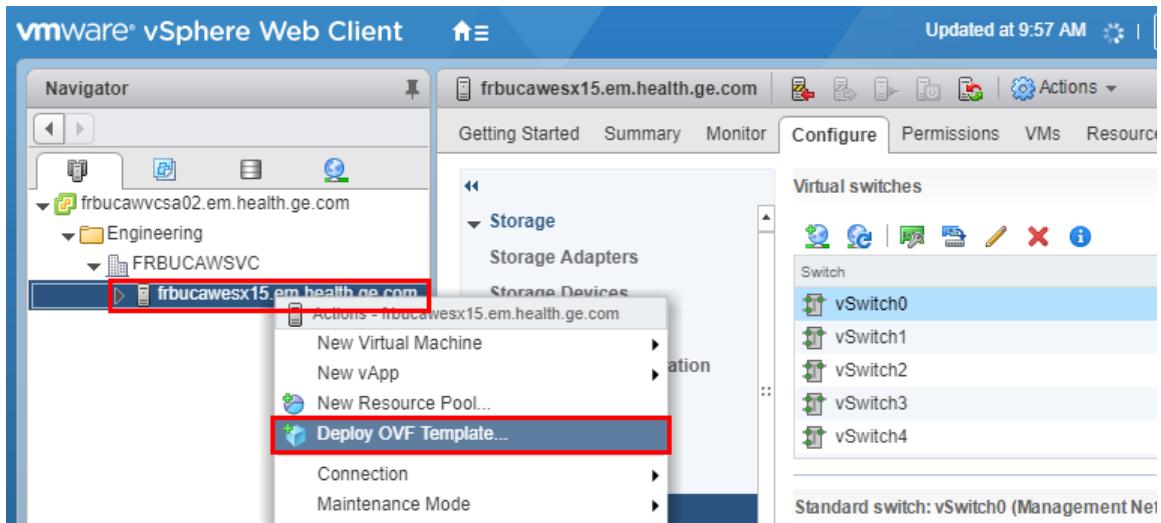
#### **IP address checklist:**

Description	IP address	Netmasks / Network pre-fix	Hostname	AE Title	DICOM Port
<b>Management network</b> (Hypervisor)		N/A	N/A	N/A	N/A
<b>vAW Server eth0</b> (hospital network)					4006
<b>PACS</b> (hospital network)		N/A	N/A		
<b>PACS</b> (hospital network) (Storage commitment)		N/A	N/A	N/A	
<b>External License server #1</b>		N/A	N/A	N/A	N/A
<b>External License server #2</b>		N/A	N/A	N/A	N/A
<b>Remote Host #1</b>					
<b>Remote Host #2</b>					
<b>Remote Host #3</b>					
<b>Remote Host #4</b>					
<b>Remote Host #5</b>					
<b>DICOM printer #1</b>					
<b>PostScript printer #1</b>					

#### **2.7.2.1 OVF Template Installation**

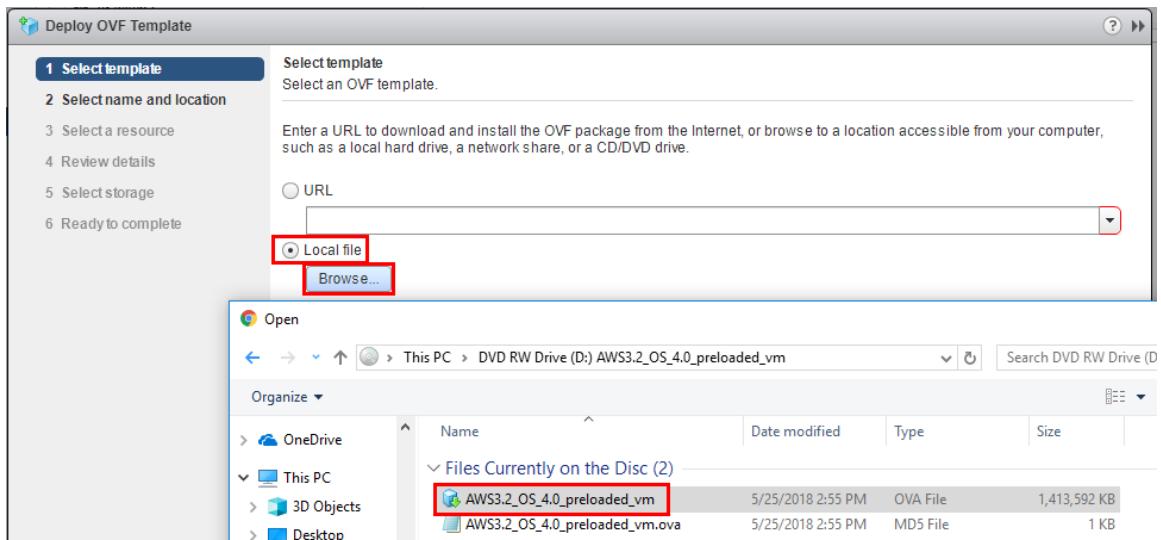
The OVF Template allows creating a VM (virtual machine) with the required characteristics (virtual memory, number of virtual CPUS, etc...) for the Low Tier AW Server, and install at the same time the Linux OS or the Linux OS + the AW Server.

1. Insert the Template media into the PC.
2. Make sure you are logged on the vSphere Web Client as **administrator**.
3. Right click on the Hypervisor and select **Deploy OVF Template...**



The *Deploy OVF Template* wizard displays.

4. Select **Local file** and click on the **Browse** button to locate the .ova file from the OVF Template media, then click on the **Open** button to select.



#### NOTE

On some media the .ova file is embedded within an .iso file. In this case, double click the .iso file to locate the .ova file.

5. Click on **Next**.

#### NOTE

The identification of the release that you want to install may be different from the one shown in the example.

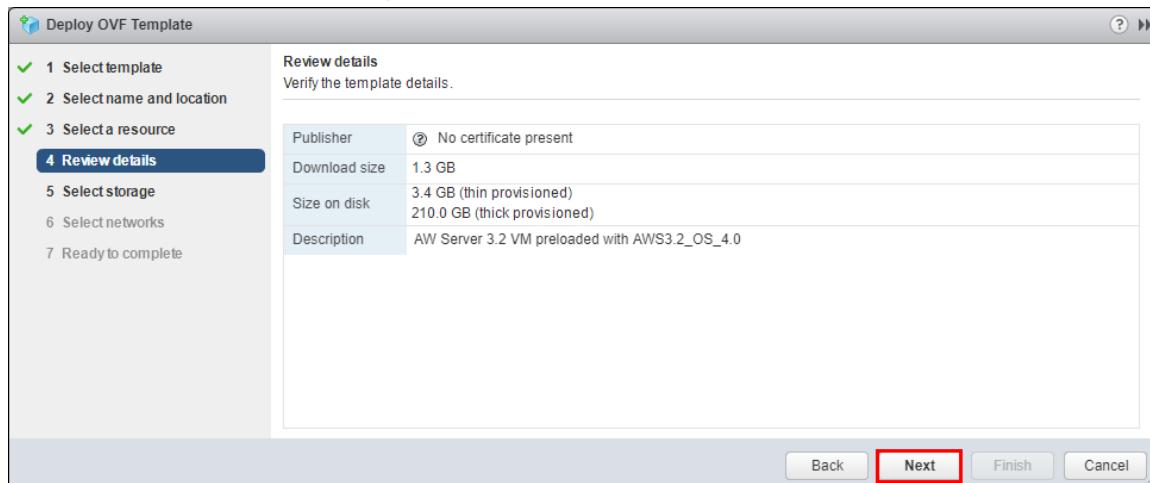
The *Select name and location* panel displays.

6. Enter a name for the Virtual Machine: i.e: **AWS3\_VM01** (for first VM) ; **AWS3\_VM02** (for next) , etc.
7. Select the datacenter where you want to deploy the OVF template.
8. Click on **Next**.

The *Select a resource* panel displays.

9. Select the Hypervisor where you want to run the deployed template.
10. Click on **Next**.

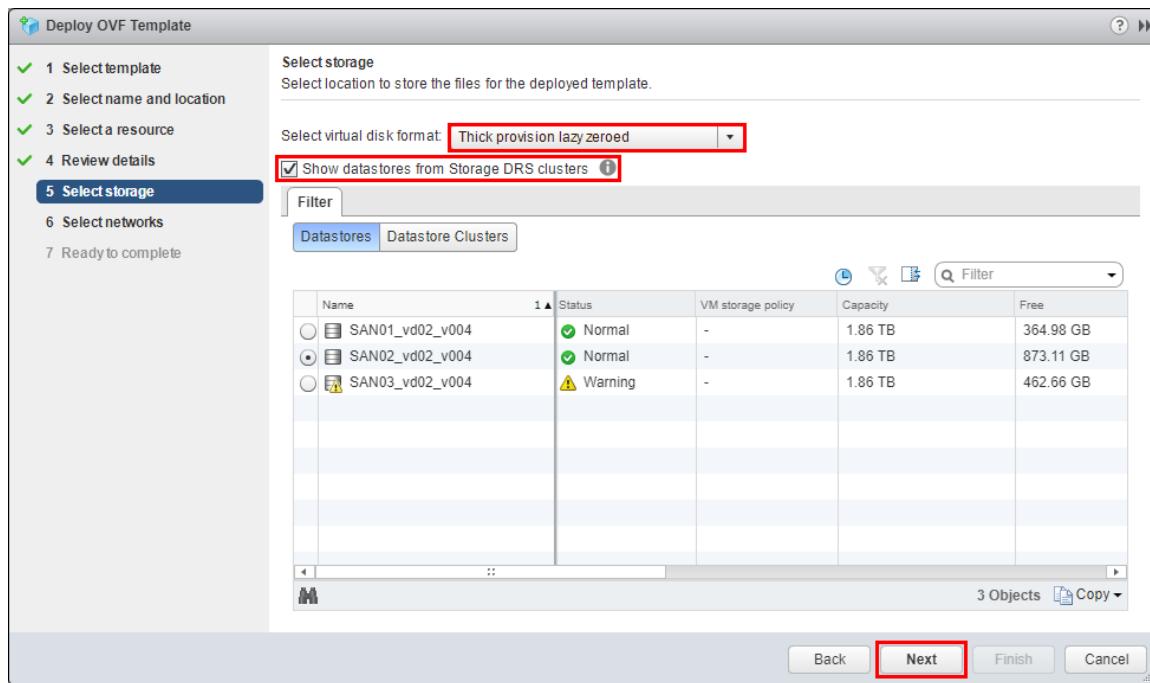
The **Review details** panel displays.



11. Click on **Next**.

The **Select storage** panel displays.

12. AW Server / HAPS server VM creation: Accept the default virtual disk format settings (**Thick Provision Lazy Zeroed**).
13. Select **Show datastores from Storage DRS clusters** check box, to be able to choose individual datastores.
14. Click on **Datastores**.
15. Choose a Datastore that will host the VM (see example below):



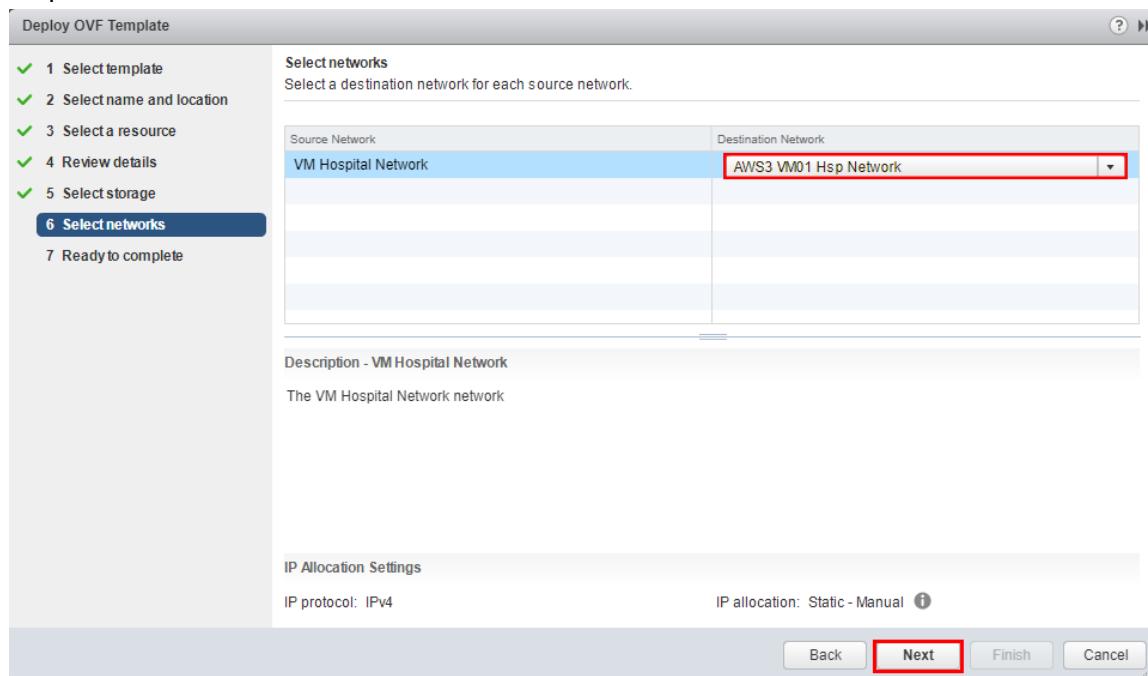
#### NOTE

For information about Disk Format, see:

[https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc\\_50%2FGUID-4C0F4D73-82F2-4B81-A7-1DD752A8A5AC.html](https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc_50%2FGUID-4C0F4D73-82F2-4B81-A7-1DD752A8A5AC.html)

16. Click on **Next**.

The **Select networks** panel displays. It allows to map the destination network for each source network.



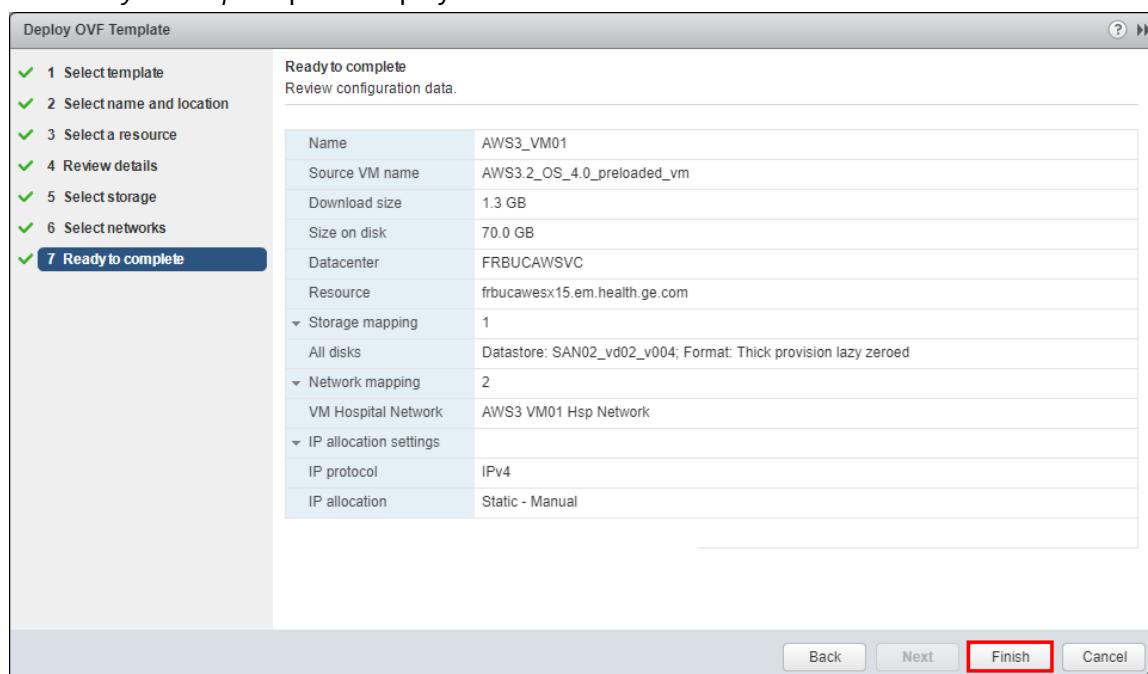
- On the **Hospital Network** line, select the Destination network from the scroll-down menu. The name of the destination network corresponds to the port group you have created or identified in [2.6.2 Ethernet ports Allocation on page 60](#) Section. As a reminder, this port group has to be associated with at least one physical network card dedicated to AW Server VM

#### 18. NOTE

You can change these parameters at a later time by editing the VM settings if needed.

Click on **Next**.

The **Ready to complete** panel displays with the Virtual Machine details.



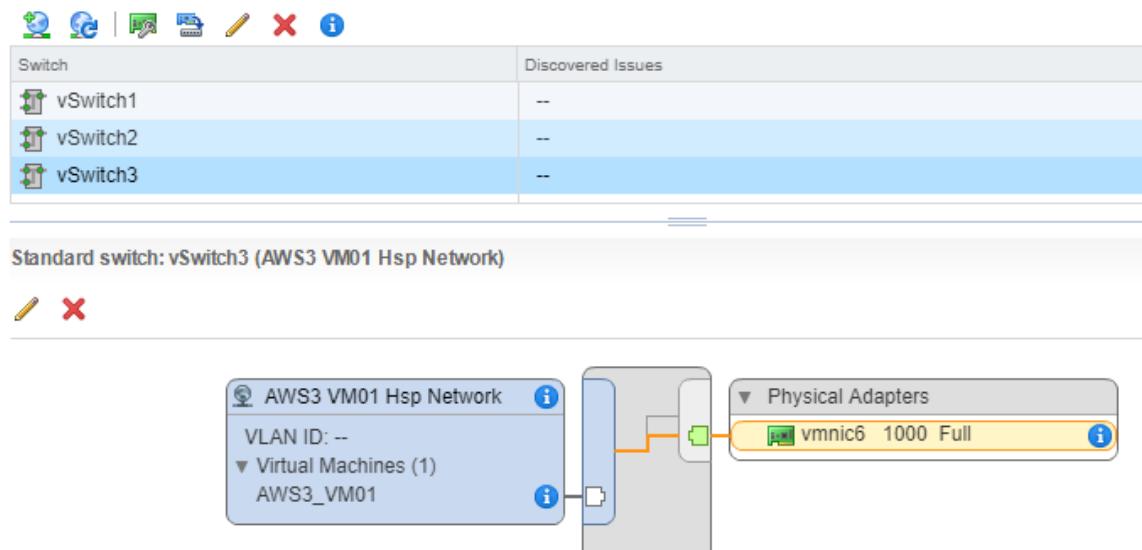
- Click on **Finish** to accept and start the VM creation.

The *Deploying OVF Template* task appears in the *Recent Tasks* section at the bottom of the page. A status bar lets you know about the deployment progress.

It will take several minutes to complete.

20. After the task status displays as **Completed**, eject the USB media and store it in a safe place.
21. Check that the Virtual Machine has been associated to the right physical network card:
  - a. Select the Hypervisor if not already done.
  - b. Click on the *Configure* tab.
  - c. Expand the **Networking** sub-menu.
  - d. Click on **Virtual switches**.

The configuration should be similar to the following:



Proceed to section [2.7.2.2 Steps to upgrade / downgrade a Virtual Machine on page 75](#).

## 2.7.2.2 Steps to upgrade / downgrade a Virtual Machine

Depending on the type of virtual AW Server purchased by the site you may have to upgrade or downgrade the virtual AW Server.

The upgrade / downgrade of a Virtual Machine consists of updating the VM memory and/or CPU. Refer to [2.4.1 Virtual AW Server Characteristics on page 36](#) to update the VM memory and/or CPU to the right values.

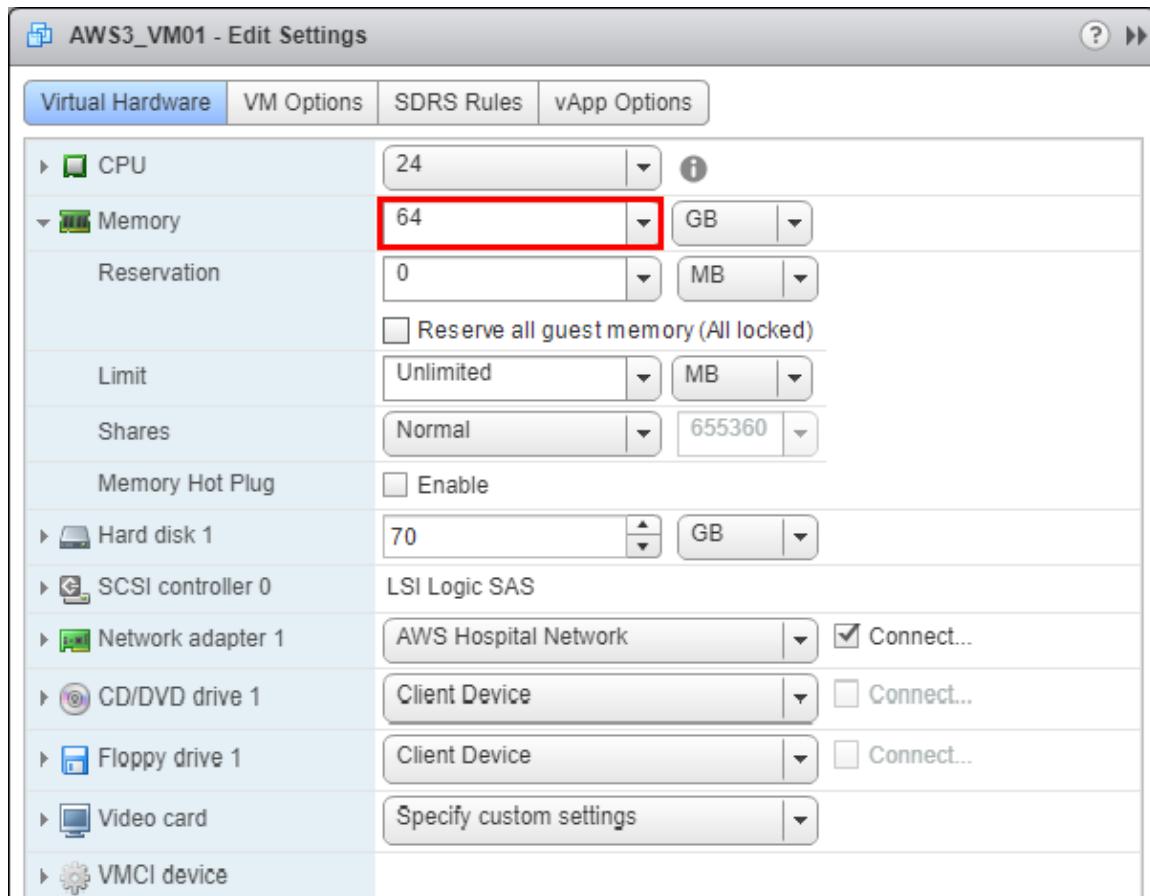
The below steps are performed for the upgrade of a Low tier VM into a High Tier VM. For the downgrade of a VM, the steps are similar.

1. Display the *Edit Settings* panel:

Right click on the Virtual Machine you have created under the Hypervisor, and that you want to upgrade / downgrade, and select **Edit settings**.

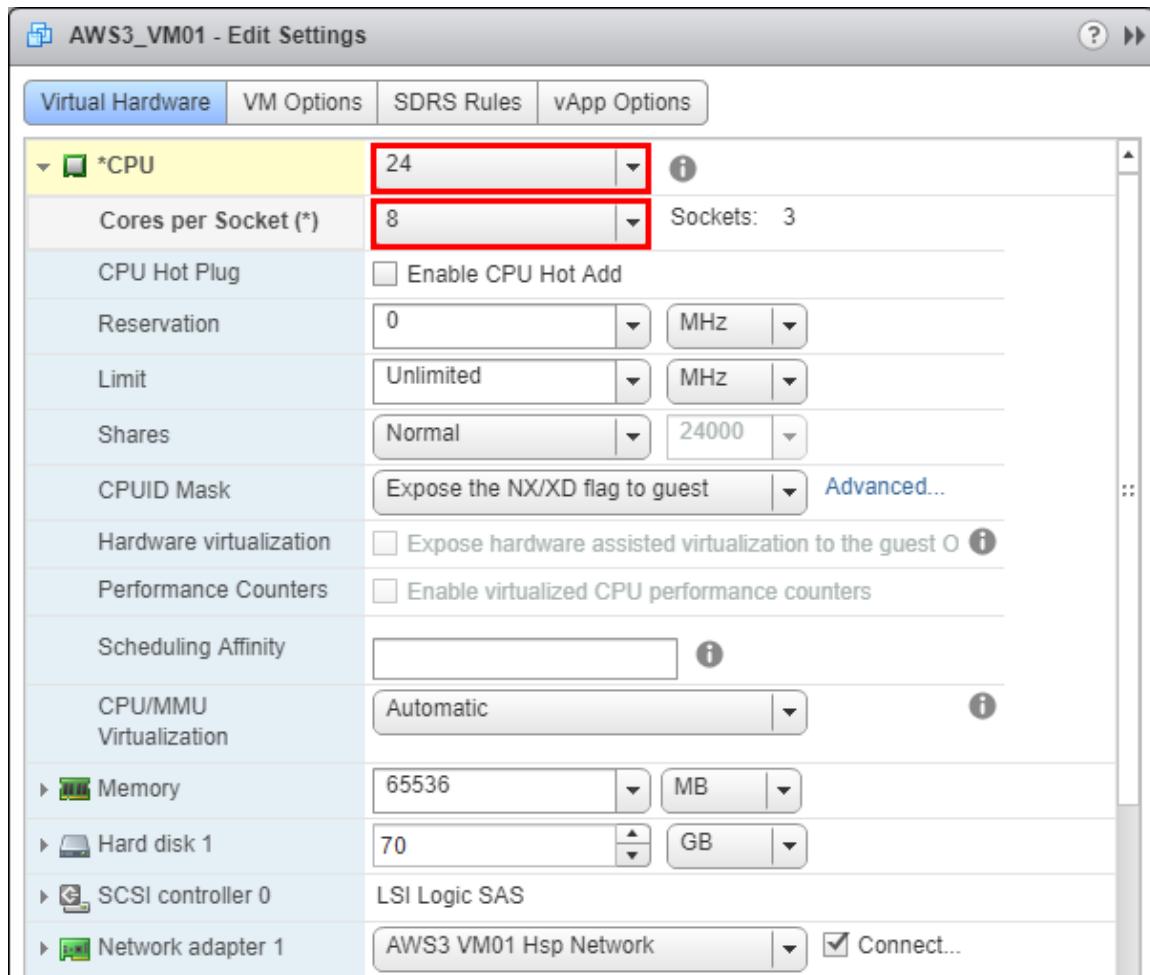
2. Update the VM memory:

In the *Virtual Hardware* tab select **Memory** from the list and set the memory size to 64GB.



3. Update the VM CPU:

In the *Virtual Hardware* tab select **CPU** from the list and set the CPU number to 24.



#### NOTE

To achieve the proper CPU number necessary to set core numbers to 24, select 3 virtual sockets and 8 core per sockets.

- Click on **OK**.

For a Standalone (Non-Integrated) virtual AW Server, proceed to section [2.7.2.3 Creating the image data disk for Standalone \(Non-Integrated\) and Hybrid AW Server on page 77](#).

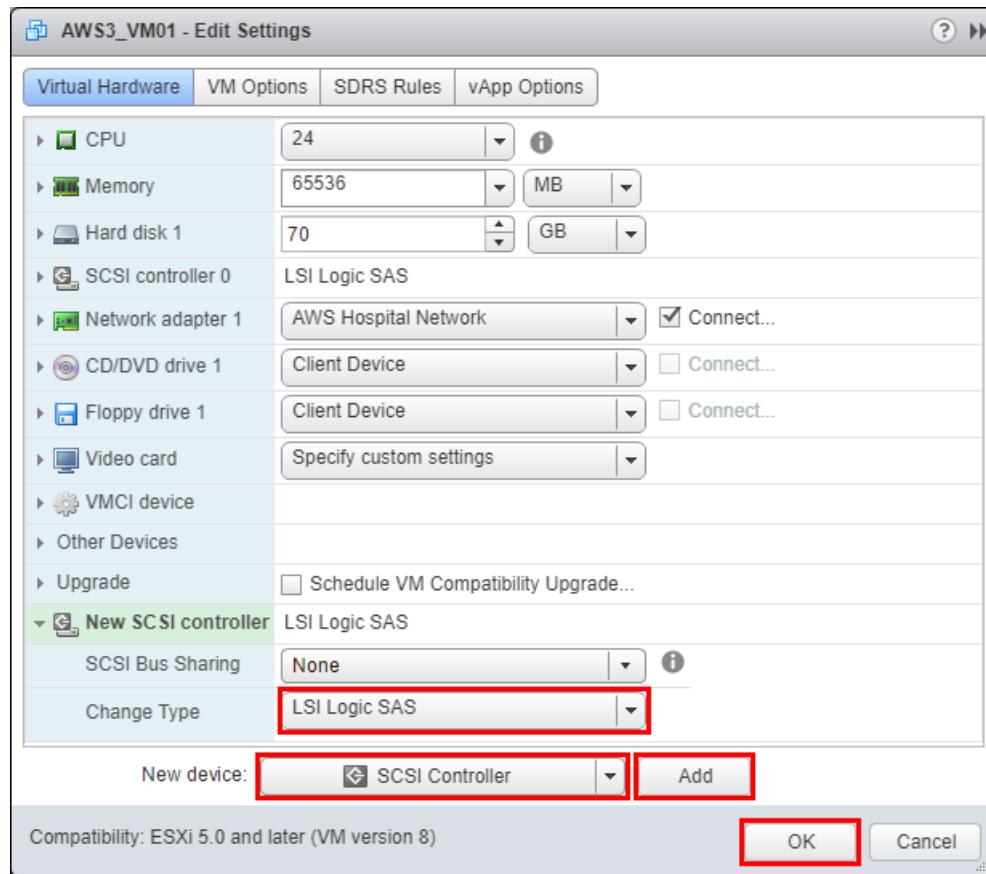
For an "integrated" virtual AW Server, proceed to section [2.9 Job Card IST002B - Virtual Machine Installation Verification on page 87](#).

### 2.7.2.3 Creating the image data disk for Standalone (Non-Integrated) and Hybrid AW Server

Perform this section if the site has purchased a Standalone (Non-Integrated) virtual AW Server. The purpose is to create a virtual hard disk partition to store the image data.

- Create a new SCSI controller. The new image data disk will have a separate SCSI controller.
  - Right click on the Virtual machine and select **Edit settings**.  
The *Edit Settings* screen displays.

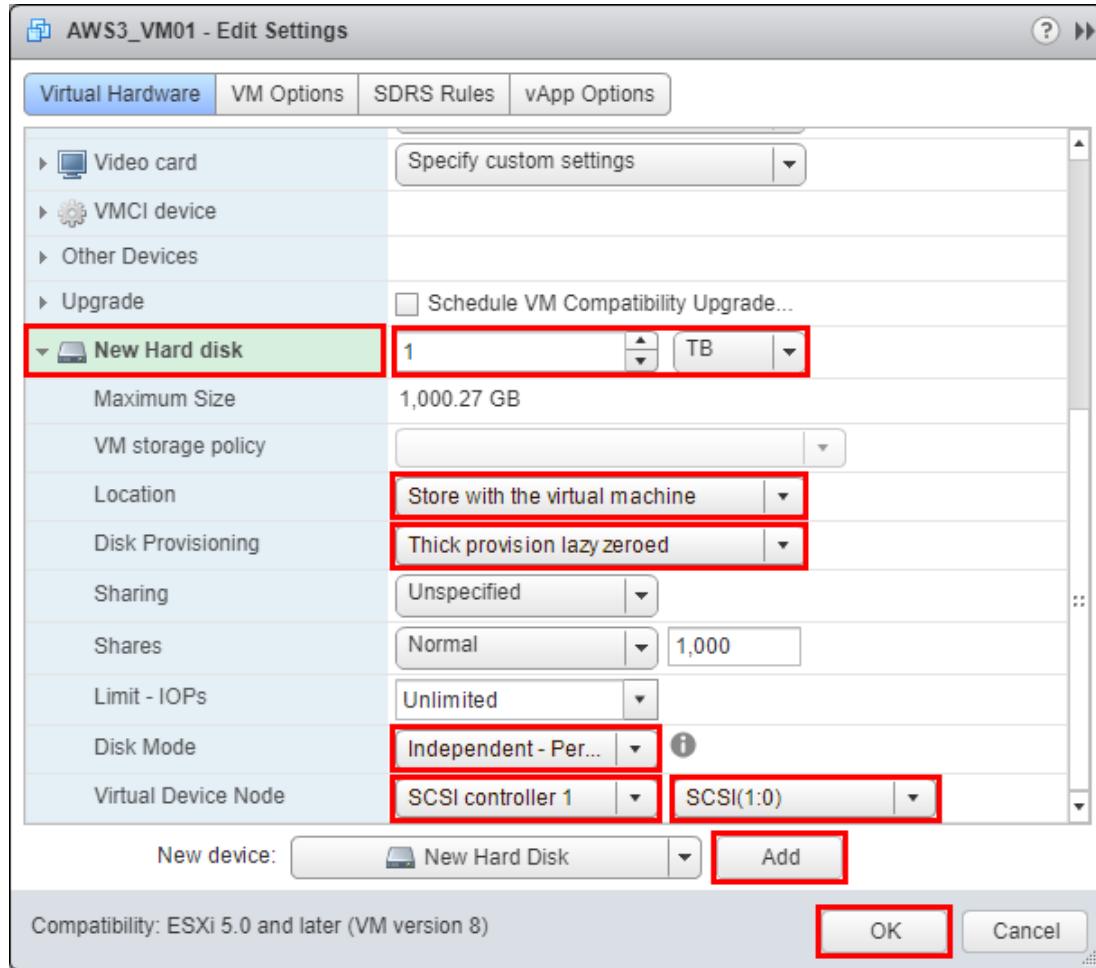
- b. In the *Virtual Hardware* tab, set **New device** to **SCSI Controller** and click on **Add**.



The **New SCSI controller** item appears.

2. Configure the new SCSI controller:
  - a. Expand the **New SCSI controller** item.
  - b. Set **Change Type** of SCSI controller to **LSI Logic SAS**.
  - c. Verify the setting and click on **OK**.
3. Create a new hard disk:
  - a. Right click on the Virtual machine and select **Edit settings**.
  - b. The *Edit Settings* screen displays.

- c. In the *Virtual Hardware* tab, set **New device** to **New Hard Disk** and click on **Add**.



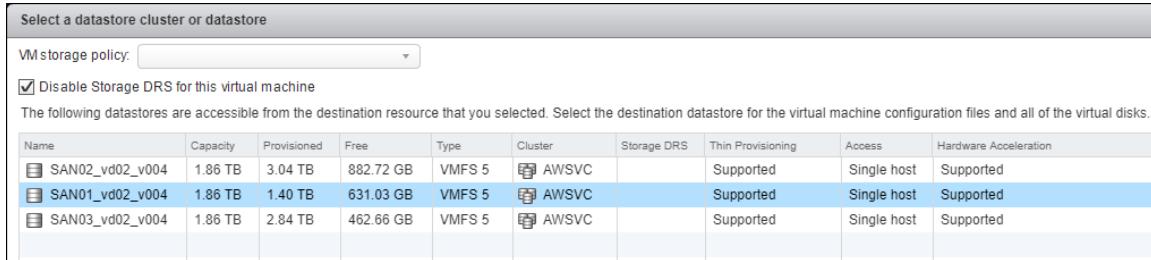
The **New Hard disk** item appears.

4. Configure the new hard disk:
  - a. Expand the **New Hard disk** item.
  - b. Set the Disk size to:
    - 1TB (minimum recommended size)
    - 6TB (recommended and maximum supported size)
  - c. Set the **Location** of disk image by selecting **Store with the virtual machine** (default setting) or select **Browse** to specify a datastore or datastore cluster (see next step).
  - d. Set **Disk Provisioning** to **Thick Provision Lazy Zeroed** (default setting).
  - e. Set **Disk Mode** to **Independent - Persistent**.
  - f. Set **Virtual Device Node** to **SCSI controller 1** and **SCSI (1:0)**. The image data disk will have a separate SCSI controller.
  - g. Verify the setting and click on **OK**.
  - h. Apply the datastore recommendations in the screen that displays.

#### **NOTE**

To help for proper choice see: [https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc\\_50%2FGUID-4C0F4D73-82F2-4B81-8A7-1DD752A8A5AC.html](https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc_50%2FGUID-4C0F4D73-82F2-4B81-8A7-1DD752A8A5AC.html).

5. When selecting a different datastore (select **Browse in Location**), the following screen appears:



- Select the **Disable Storage DRS for this virtual machine** check box.
  - Select the appropriate datastore.
  - Click on **OK**.
6. Right click on the Virtual machine and select **Edit settings**.

In the *Virtual Hardware* tab, now you can see a new SCSI Controller and a new Hard Disk. This completes the installation of the Virtual machine.

Proceed to [2.9 Job Card IST002B - Virtual Machine Installation Verification on page 87](#).

## 2.8 Job Card IST001C - Virtual Servers Cluster Installation Steps

### 2.8.1 Foreword

Scalability mode (or cluster mode) is the ability to have several AW Servers working as one more powerful AW server (currently limited to a maximum of “virtual” AW Servers). The behavior is “transparent” for the user, who will be automatically directed to the appropriate server (less loaded) when logging in.

If your site is going to have a cluster of two or more virtual AW servers, you need to set up each of the servers in the "Cluster mode". Proceed as follows and repeat this operation on each of the other virtual AW servers.

**Currently, the Scalable mode is only supported with virtual AW Servers.**

#### 2.8.1.1 Pre-requisites for Cluster operation

The following are pre-requisites for proper operation of Scalability. However the AW Servers can be setup for Scalability before the pre-requisites are met, but will not behave as so until the pre-requisites are met.

- Two HAPS (High Availability Preferences Sharing) nodes shall be created within the cluster, in order to host and share between the AW Servers, the Preferences created by the users.
- The AW Servers shall be fully licensed.
- All AW Servers in the cluster must run the same SW version for both:
  - The AWS platform software
  - The Applications software

These conditions are checked by the "Golden set" feature, and cluster operation will not be permitted if those conditions are not met.

- The same Applications are licensed and installed on all AW servers of the cluster. Refer to [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#).

- Pre-processing is optional. If it has been purchased for the site, it shall be available and configured for each AW Server in the cluster (same pre-processing configuration for all AW Servers).
- All AW Servers in the cluster must share the same Image database. Therefore, the AW Servers shall be setup for **Seamless** and **DICOM Direct Connect integration** with the PACS. Refer to [2.19 Job Card IST011 - Integration on page 221](#).
- The License server(s) is/shall be configured and alive - preferably use external license servers to avoid using one of the AW Servers as License server.

#### NOTE

It is not necessary that each AW Server in the cluster is declared to the other nodes as a DICOM host.

## 2.8.2 Preliminary Steps

The GEHC FE delivers the media necessary for installation to the IT administrator of the site.

All along this section, you will refer to [2.7 Job Card IST001B - Virtual Machine creation on page 68](#) - to setup each virtual servers (AW Servers + 2 HAPS servers) that constitute the cluster.

### 2.8.2.1 Virtual machine resources for AW Server

#### 2.8.2.1.1 High Availability Preferences Server (HAPS)

Thanks to the OVF Template OS media, a standard virtual machine for AW Server Low Tier will be created, from which the virtual machine for HAPS Server will be downgraded in order to meet the necessary resources to run HAPS Node:

- processor: 2 vCPUs
- disk: one 210GB virtual HDD
- memory: 4GB
- network: One physical Ethernet port

#### 2.8.2.1.2 AW Server

Thanks to the OVF Template OS media, the standard virtual machine for AW Server Low Tier will be created with the necessary resources to run AWS Node:

- processor: 8 vCPUs
- disk: one 210GB virtual HDD
- memory: RAM depends on integration mode, see table in section [2.4.1 Virtual AW Server Characteristics on page 36](#)
- network: One physical Ethernet ports (1 Ethernet used for customer network)

### 2.8.2.2 Physical Network configuration

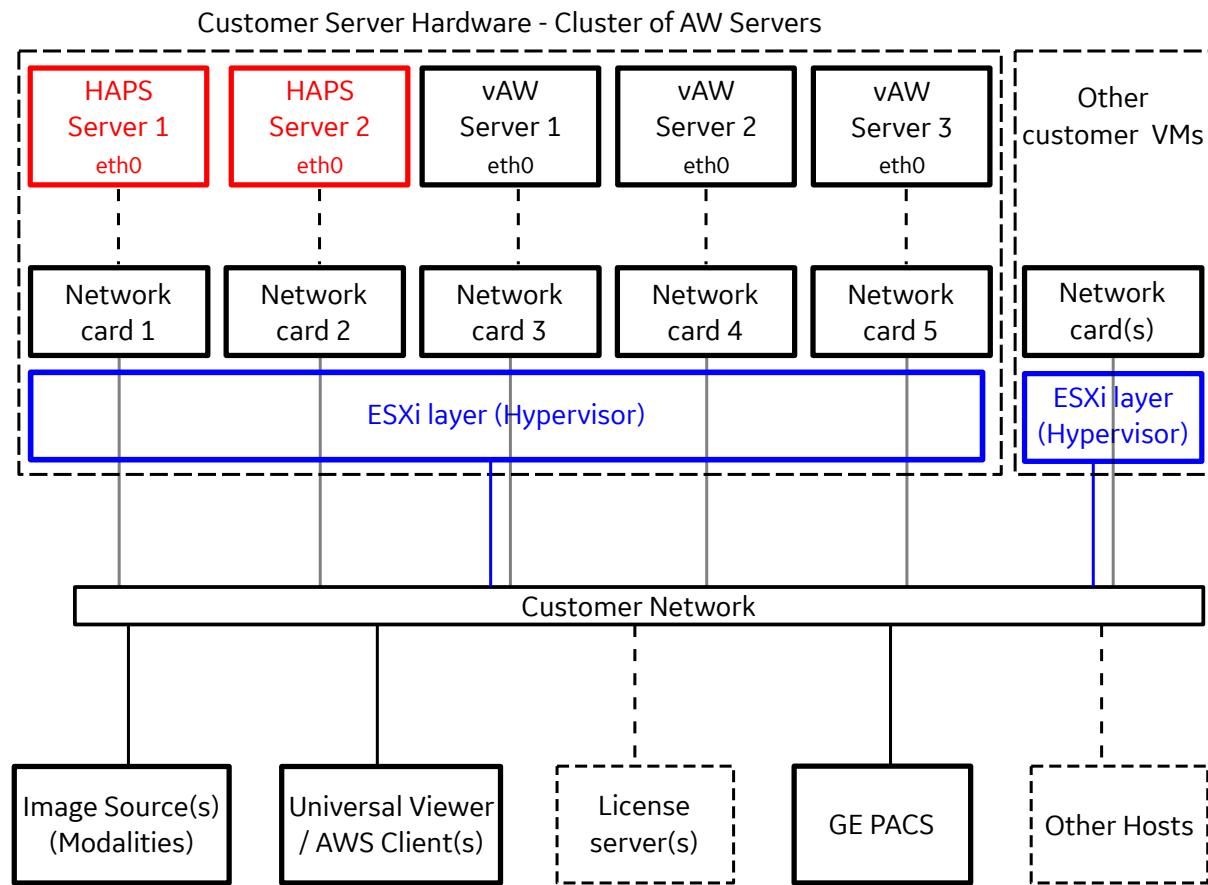
Each virtual **AW Server** as well as each virtual **HAPS Server** must be linked to **one** 1Gbps physical network card (Ethernet port) to ensure proper operation.

The 1GB/s physical network card is dedicated to the AW Server, for communication with the other hosts and for communication with other nodes (AW Servers) and HAPS within the cluster, on the Hospital network (VM Hospital Network).

**NOTE**

It is recommended to use a separate NIC for the Management network of the Hypervisor, in order to ensure that enough bandwidth will be available during template deployment or other similar operations.

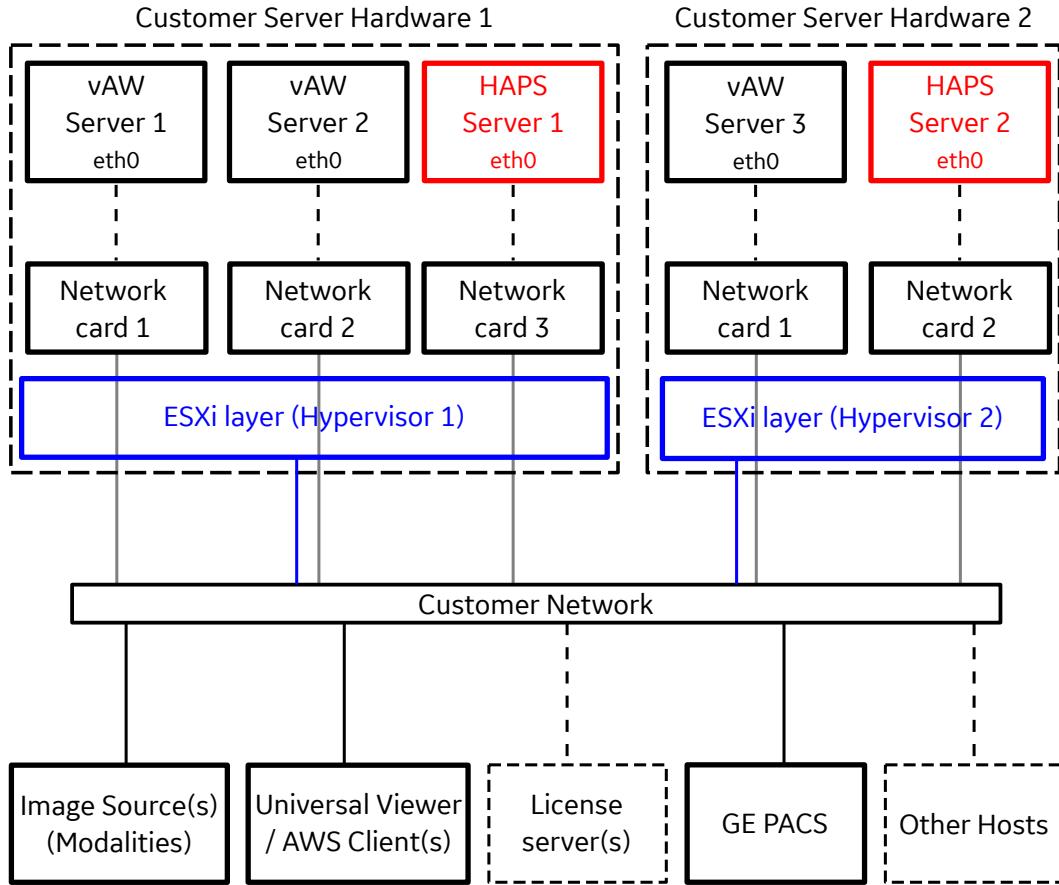
**Figure 2-4 Example of cluster of 3 virtual AW Servers hosted on the same physical server**

**NOTICE**

Two HAPS (High Availability Preferences Sharing) servers VM shall be created through the OVF Template OS and the AWS Platform software.

**NOTICE**

In order to ensure proper hardware redundancy, it is strongly recommended that the two HAPS servers are hosted on different Hypervisor hardware (see hereafter).

**Figure 2-5 Example of a cluster of 3 virtual AW Servers hosted on two different servers hardware**

The cluster can be distributed on several hospitals (the second customer server hardware can be in another hospital).

#### **NOTE**

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

## **2.8.3 Installation and configuration Steps**

The following sections are already described in details in the Job Cards [2.6 Job Card IST001AB - Hypervisor Configuration on page 59](#) and [2.7 Job Card IST001B - Virtual Machine creation on page 68](#). Therefore all the steps are not repeated hereafter, but you will be directed to the appropriate section of these Job Cards which contains the necessary information for the setup.

### **2.8.3.1 Hypervisor pre-requisites**

One Hypervisor must be installed per server hardware aimed to host the virtual machines.

All hypervisors must run the same software version.

**This step is under the full responsibility of the IT administrator of the site.**

### 2.8.3.2 Ethernet ports allocation

For each hypervisor that will host the virtual AW Server, there is one physical network card dedicated to the AW Server VM.

**This step is under the full responsibility of the IT administrator of the site.**

Refer to [2.6.2 Ethernet ports Allocation on page 60](#).

### 2.8.3.3 GE Service account setup

A GE Service account must be created so that the GEHC FE has all necessary permissions to administrate each virtual machine hosting a virtual **AW Server** and/or a **HAPS server**.

**This step is under the full responsibility of the IT administrator of the site.**

Refer to [2.6.3 Create a GEHC service user account on page 63](#).

### 2.8.3.4 NTP server setup for the Virtual AW Servers / HAPS servers

Time synchronization through a NTP server is a “must” for scalability. The NTP server must be setup for each virtual machine hosting a virtual AW Server or a HAPS server.

**This step is under the full responsibility of the IT administrator of the site.**

Refer to [2.6.4 Setup a NTP server for the Hypervisor on page 67](#).

### 2.8.3.5 Virtual Machine (VM) creation

Each VM aimed to host one virtual AW Server must be created from the OS (OVF) Template media.

**This step is under the full responsibility of the IT administrator of the site.**

Refer to [2.7 Job Card IST001B - Virtual Machine creation on page 68](#).

### 2.8.3.6 AW Server / HAPS server installation and configuration

Once each virtual machine has been created by the IT administrator of the site, and a GE Service account is available to administrate each virtual machine, the GEHC FE will load and configure (if not already done during VM creation) either the HAPS server software or the AW Server. Then he/she will verify the VMs created and finally load the Applications software.

**These steps are under the full responsibility of the GEHC FE.**

## 2.8.4 Scalability Installation Checklist

### 2.8.4.1 Under Site IT administrator responsibility

1. Allocate the Network resources.

Refer to section [2.6.2 Ethernet ports Allocation on page 60](#).

Make sure one physical network port is available for each VM (AW Server and HAPS server for the hospital network).

2. Setup a GE Service account with appropriate permissions to administrate the HAPS and AW Server VMs.

Refer to [2.6.3 Create a GEHC service user account on page 63](#).

3. Make sure the NTP server is up and running.

Refer to [2.6.4 Setup a NTP server for the Hypervisor on page 67](#).

#### 4. Virtual Machines creation.

Refer to [2.7 Job Card IST001B - Virtual Machine creation on page 68](#).

- a. Create the HAPS Server 1 VM from the OVF template.
- b. Downgrade the VM to match HAPS VM characteristics.
- c. Create the HAPS Server 2 VM from the OVF template.
- d. Downgrade the VM to match HAPS VM characteristics.
- e. Create the AW Server 1 VM from the OVF template.
- f. Create the AW Server 2 VM from the OVF template.
- g. Create the AW Server n VM from the OVF template.

### 2.8.4.2 Under GEHC FE responsibility

#### 1. VM creation verification:

Refer to [2.9 Job Card IST002B - Virtual Machine Installation Verification on page 87](#).

- a. Login with the GE service account credentials.
- b. Start and verify the AW Server and HAPS VMs.

#### 2. HAPS Platform software installation:

Refer to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#).

- a. From the AWS platform media, install HAPS server 1 and setup Network and Time parameters.
- b. From the AWS platform media, install HAPS server 2 and setup Network and Time parameters.

#### 3. AWS platform software installation:

##### NOTE

Perform this step only if the AW Server Platform Software is **not** already installed within the OVF Template (USB media).

Refer to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#).

- a. From the AWS platform media, install AW Server #1 and setup Network and Time parameters.
- b. From the AWS platform media, install AW Server #2 and setup Network and Time parameters.
- c. From the AWS platform media, install AW Server #n and setup Network and Time parameters.

#### 4. Installation Wizard:

##### NOTE

Perform this step if the AW Server Platform Software is already installed within the OVF Template (USB media).

Refer to [2.10 Job Card IST002C - Installation Wizard - Prepare and perform the AW Server configuration on page 90](#).

- a. From the USB media, launch the Installation Wizard to prepare and create the AW Server 1 configuration. Then configure AW Server 1 using Cloud-Init mechanism.
- b. From the USB media, launch the Installation Wizard to load the AW Server 1 configuration as a template. Then update the configuration for AW Server 2. And finally, configure AW Server 2 using Cloud-Init mechanism.

- c. From the USB media, launch the Installation Wizard to load the AW Server 1 configuration as a template. Then update the configuration for AW Server n. And finally, configure AW Server n using Cloud-Init mechanism.
5. Login to and configuration of the AW Servers.
  - For Seamless Integration: Dakota plugin loading: Refer to [2.19 Job Card IST011 - Integration on page 221](#).
  - Initial Configuration: Refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#).
6. Load and install the Applications:  
Refer to [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#).  
Load and install the VW Apps Applications from media.
7. Integration configuration:  
Refer to [2.19 Job Card IST011 - Integration on page 221](#)
  - a. Configure integration on the AW Server side.
  - b. For Seamless Integration: Configure integration on the UV side.
8. Administrative configuration:  
Refer to [2.18 Job Card IST010 - Administrative Configuration on page 184](#).
  - a. Configure remote hosts and printers (if applicable).
  - b. Configure Users.
  - c. Configure Pre-processing and End Of Review.
9. Service Tools configuration:  
Refer to [2.22 Job Card IST013 - System Configuration Registration on page 259](#).
  - a. Register Configuration and obtain the registration key.
  - b. Exit the Maintenance mode.
10. Scalability configuration:  
Refer to [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#).
  - a. Certificate Management: In order for the nodes (AW Servers) and the HAPS to communicate securely between them, generate certificates and deploy them on the nodes and the HAPS.
  - b. Check the cluster configuration and that the HAPS are up and running.
  - c. Configure the Goldenset.
11. Client install:  
Refer to [2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282](#).
  - a. Download and Install the Solomini client.
  - b. Launch the Universal Viewer and create a 3D Apps button (for Seamless integration).
  - c. Launch the AW Server Client / 3D applications.
12. Final steps:
  - Refer to [2.27 Job Card IST015 - Final Settings on page 292](#).
  - Refer to [2.28 Job Card IST016 - System Handover to Customer on page 298](#).

## 2.9 Job Card IST002B - Virtual Machine Installation Verification

This Job Card **only applies for Virtual servers** installed by the IT administrator of the site.

It DOES NOT apply for the hardware based AW Server (refer to [2.5 Job Card IST001A - Hardware Installation Verification on page 45](#)).

**The steps described in this Job Card shall be completed under the full responsibility of the GEHC FE for each Virtual machine created.**

### NOTICE

#### \*\*\* IMPORTANT PROCESS REQUIREMENT \*\*\*

- Any deficiencies or hardware failures found while executing the following verification process must be IMMEDIATELY reported to the GEHC OLC support team and the site IT admin, to be resolved prior to GEHC Service accepting ownership of the system, and installing the AW Server software!!!
- Additionally, the GEHC FE is required to overlap with the IT administrator of the site during these final checks to also observe and ensure proper hardware readiness.
- In an event requiring the IT administrator of the site to resolve an installation hand-off problem, the GEHC FE should "break off" and not log the IT administrator resolve time against the GEHC installation. Training time can be logged if the GEHC FE desires to observe – but not actual installation time until the hand-off is successful.

### Time Reporting for Installation & Warranty

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

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

#### Virtual AW server - 5 to 8 hours, with:

- 1 to 2 hours for the VIRTUAL machine creation (incl. OS load) by the IT admin of the site
- 4 to 6 hours for the AWS Software / Configuration (GEHC) installation.

This includes one hour of overlap time for the GEHC FE to engage the IT admin, and to acquire site readiness and installation status information.

- Charge any system malfunction / troubleshooting and repair time to the appropriate warranty service class (10 or 11).

### NOTICE

When a Virtual Machine (VM) is created, a MAC address is automatically created for this VM. From this MAC address, the "Licenseld" is created, that will be used to calculate from the eLicense web site the license keys for the AW Server platform, Integration, Pre-processing option, Applications, etc...

This VM and MAC address creation happened while loading the OS from the OS OVF Template media. Therefore the VM must never be deleted, otherwise the MAC address will be lost, and consequently the keys for all AWS applications.

That is the reason why you are provided with the OS media for Virtual machine - To be used to reload the OS in case it will be necessary to do so.

## 2.9.1 Retrieving the MAC address

This section describes how to retrieve the MAC address of a Virtual Machine from the ESXi Web Interface.

### NOTE

In case of configuration the AW Server with Installation Wizard, do NOT start the VM.

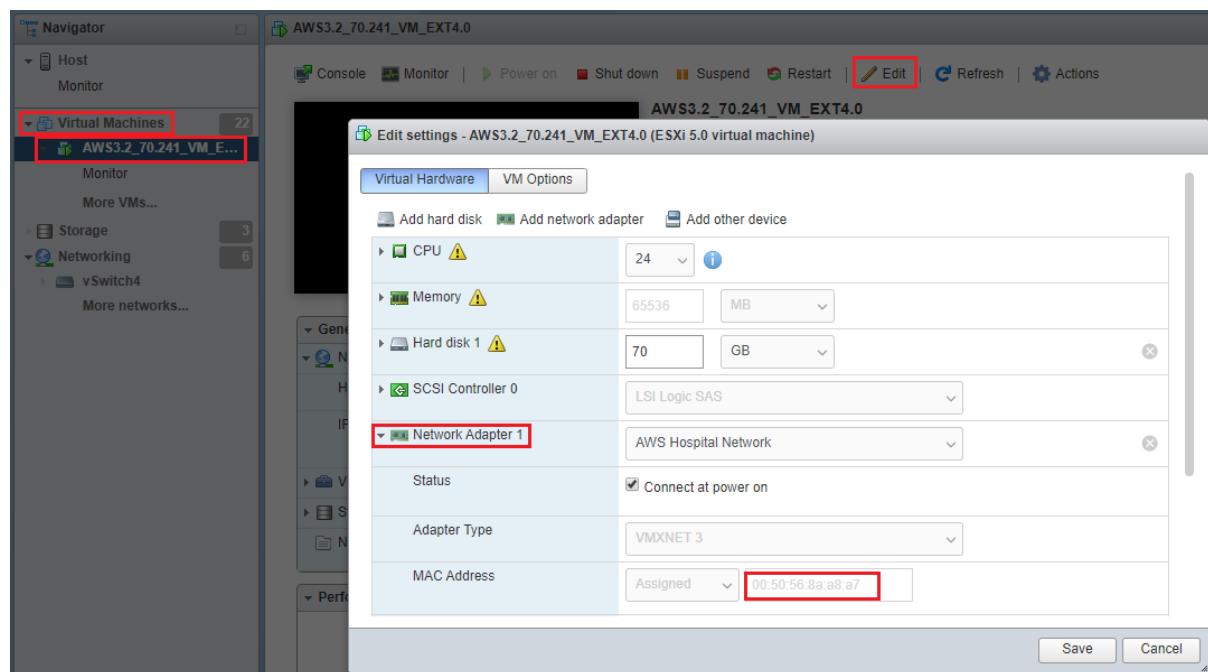
A MAC address shall be of the form XX:XX:XX:XX:XX:XX. I.e: 00:01:0c:07:ac:88

### NOTE

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

1. Connect to the *ESXi Web Interface*. In the *ESXi Web Interface* login screen (<https://<ESXi URL or IP>/>), login as **service**.
2. Click on **Virtual Machines** on the left side of the page and click on the virtual machine name in the list of virtual machines that displays.
3. Select the  **Edit** icon.
4. In the *Edit settings* screen, expand the **Network Adapter 1** item to display the MAC address.



Note the MAC address. It is requested to:

- Configure the AW Server using the Install Wizard.
- Enter the eLicense web site and calculate the keys associated to your GON (Global Order Number). Refer to [A.3 Licensing on page 556](#) for more information on eLicense, or wait until the AW Server platform software has been loaded to access to the HealthPage and/or use the command **licenseId** to display the license ID.

## 2.9.2 Verifying the Virtual Machine

### NOTE

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

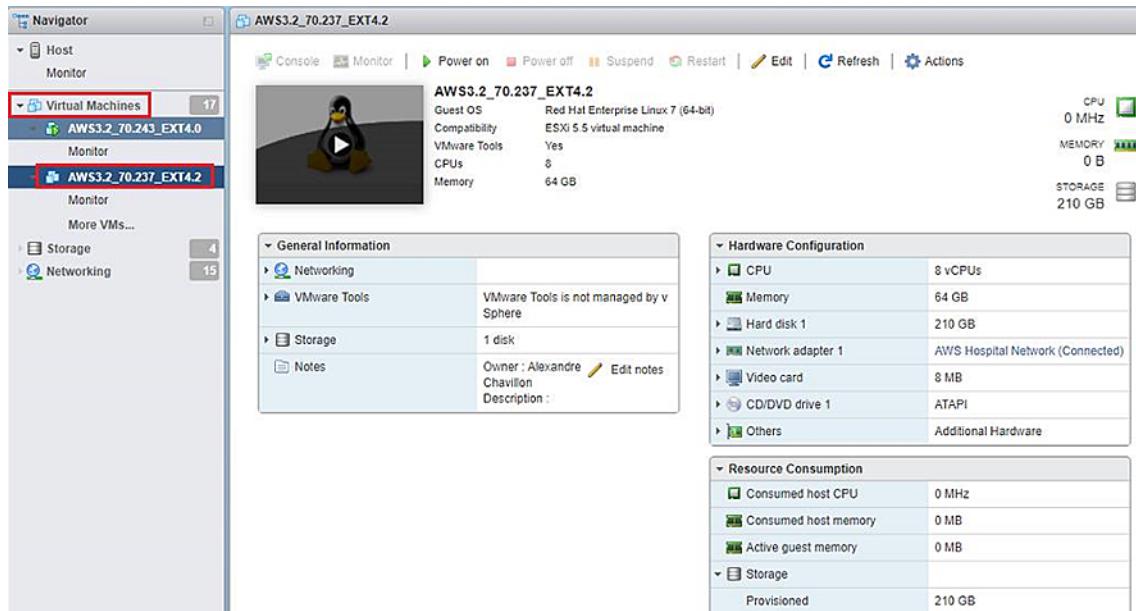
The following steps shall be done at the Client PC.

1. Connect to the *ESXi Web Interface*. In the *ESXi Web Interface* login screen (<https://<ESXi URL or IP>/>), login as **service**.

The *ESXi Web Interface* page displays.

2. Display the virtual machine's characteristics:

- a. Click on **Virtual Machines** on the left side of the page.
- b. Click on your virtual machine name in the list of virtual machines that displays.



The IT admin may have changed the default VM name to any name at their convenience, especially if there are several virtual AWS on the same server hardware.

If needed, right click on the virtual machine name and select **Rename** to change the VM name.

3. Check that the following virtual machine's characteristics are as defined in the tables of [2.4.1 Virtual AW Server Characteristics on page 36](#):
  - The Virtual CPU.
  - The Virtual memory.
  - The Virtual hard disk.
  - The second virtual hard disk for the images filesystem.

### NOTE

This second virtual hard disk is required only for No-Integ (Standalone) and Hybrid AW Server to store the images. If missing to create this virtual hard disk, create it now as described in [2.7.2.3 Creating the image data disk for Standalone \(Non-Integrated\) and Hybrid AW Server on page 77](#).

Memory overhead and Storage parameters values change from one configuration to another.  
Refer to [2.4.1 Virtual AW Server Characteristics on page 36](#).

This completes the Virtual machine installation verification.

If the AW Server Platform Software is already installed within the OVF Template (USB media) proceed to [2.10 Job Card IST002C - Installation Wizard - Prepare and perform the AW Server configuration on page 90](#)

Otherwise, proceed to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#).

## 2.10 Job Card IST002C - Installation Wizard - Prepare and perform the AW Server configuration

### 2.10.1 Overview

This Job Card applies **only for Virtual AW Server**.

**All steps are performed and completed by the GE FE.**

The Installation Wizard allows preparing and performing the basic AW Server configuration for the **DICOM Direct Connect integrated AW Server (not for HAPS)**.

It generates a configuration file that can be interpreted by the AW Server to perform the configuration automatically during its first start (it uses the Cloud-Init mechanism).

### 2.10.2 Preparing the AW Server configuration

This section describes the preparation of the basic AW Server configuration and the configuration file creation using the Installation Wizard.

The steps are done at the FE laptop.

#### 2.10.2.1 Launching the Installation Wizard

The Installation Wizard is delivered either:

- In the [Physical Software Kit on page 23](#). Use the following file:

Part Number	Content	Purpose	Integration Mode
5818084-10 (or higher) 	<code>startinstallwizard.bat</code> or <code>startinstallwizard.sh</code>	These scripts are used for <b>Initial Installation</b> to prepare the AW Server configuration (on Windows or on Linux).	DDC

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use the following file to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	Integration Mode
<code>5865572-5_AW_Server_3.2_Ext.4.9_VM_Install_Wizard.zip</code>	This compressed package is used for <b>Initial Installation</b> to prepare the AW Server configuration.	DDC

#### NOTE

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

- Insert the USB media into a USB port of the PC.

2. Double click on `startinstallwizard.bat` for Windows or `startinstallwizard.sh` for Linux.

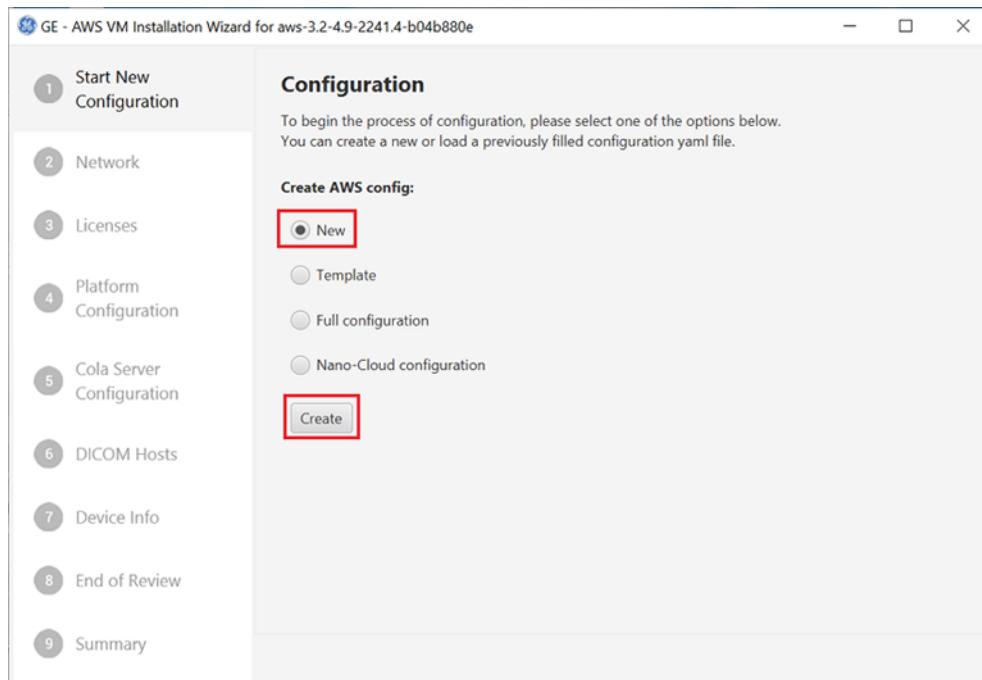
The Installation Wizard appears.

## 2.10.2.2 Starting the Installation Wizard configuration

In the **Start New Configuration** tab of the Installation Wizard, you can create a new configuration, load a configuration from a template or edit an existing configuration.

1. To create a new configuration:

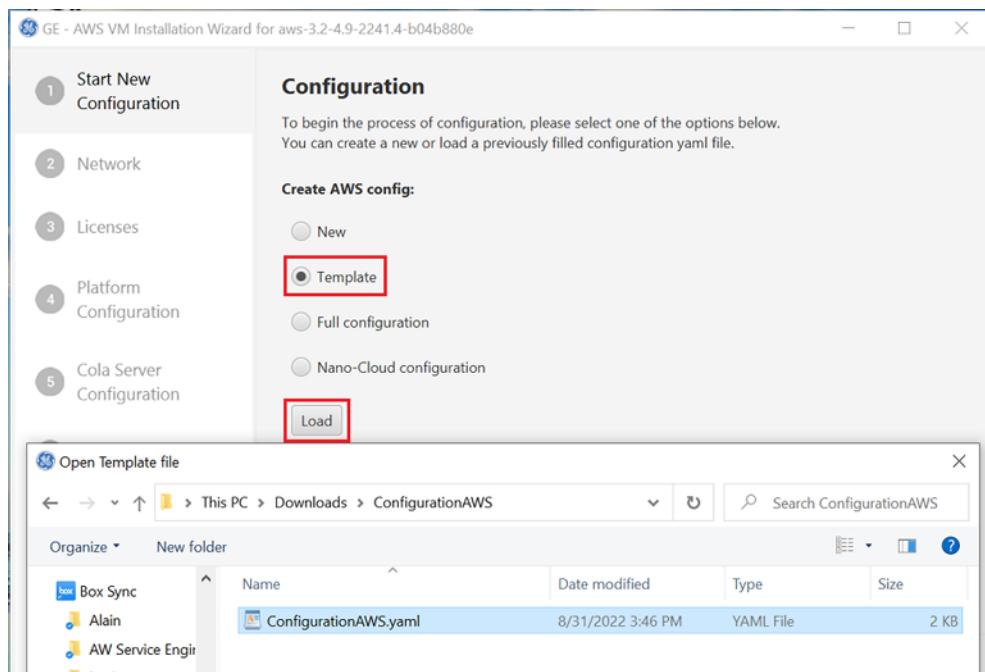
- a. Select **New**.
- b. Click on **Create**.



2. To load an existing configuration from a template:

- a. Select **Template**.
- b. Click on **Load**.
- c. Select the configuration file.

- d. Click on **Open** to load the file.



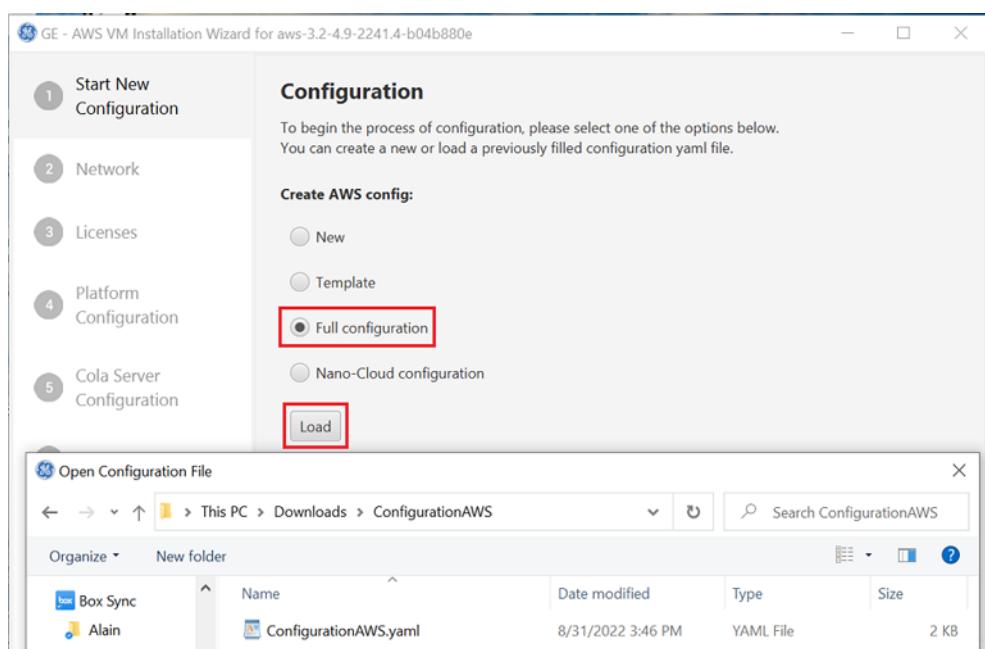
#### NOTE

All fields specific to an AW Server instance (IP, SystemID, licenses,...) are cleared.

#### NOTE

In case of cluster mode, speed up the current node (AW Server) configuration by loading the first node configuration (the node should be fully configured) as a template.

3. To edit an existing configuration:
  - a. Select **Full configuration**.
  - b. Click on **Load**.
  - c. Select the configuration file.
  - d. Click on **Open** to load the file.



**NOTE**

All fields are loaded from this file. You can update them if needed.

### 2.10.2.3 Installation Wizard navigation and Field Filling Rules

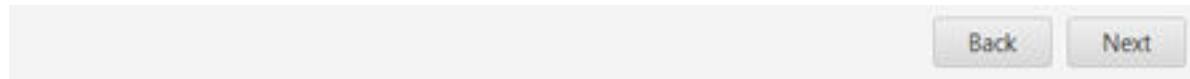
In the following steps all fields marked with an asterisk (\*) are mandatory and must be filled out. Other fields are optional.

If a field is wrongly filled, the symbol  appears next to the field and also on the corresponding tab and the *Summary* tab, as shown in the example below.

When all the mandatory fields are correctly filled, a green check appears near the fields and on the tab, as shown in the example below:

 Network	Set up network interfaces: Host name*: awsnano ✓ Domain name: IP*: 192.168.1015  Network prefix*: 24 ✓	 Network	Set up network interfaces: Host name*: awsnano ✓ Domain name: IP*: 192.168.101.5 ✓ Network prefix*: 24 ✓
Field wrongly filled (here the IP field)		Field correctly filled	

To navigate through the tabs click directly on the tab or on the **Next** and/or **Back** buttons at the bottom right of the Installation Wizard.

**NOTE**

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#), to know the characters rules and limitations of the specific fields (Hostname, AE Title, IP Address, Port, System ID, Label/Name).

## 2.10.2.4 Configuring the network and time settings

- Get all network information from the IT Admin.

**Network Configuration**

Please fill the information below about your VM's network and time settings.  
Please note:  
The MAC address shall be retrieved from the created VM.  
Changing the MAC address will clear all the previously filled license information.  
When adding multiple NTP Server the first one in the list will be used.  
Ntp server is case insensitive and it is mandatory when cluster mode is enabled.

**Set up network interfaces:**

Host name*	bucaw70-240	✓
Domain name:		
IP*:	3.249.70.240	✓
Network prefix*:	23	✓
Gateway:	3.249.71.250	✓
DNS 1:	10.220.220.220	✓
DNS 2:	10.220.220.221	✓
MAC address*:	00:50:56:8a:5d:49	✓

**Time settings:**

Region:	Europe	
City:	Amsterdam	
NTP server*:	3.40.208.30	Add

- In the **Network** tab of the Installation Wizard, enter the **Host name**.
- Enter the **IP** address, the **Network prefix** and the Default **Gateway**.
- If applicable, enter the parameters for the **DNS** server(s).
- Enter the **MAC address**.  
Refer to [2.9.1 Retrieving the MAC address on page 88](#).
- In the *Time settings*, select the **Region** and **City**.
- Enter the **NTP server**'s IP address.

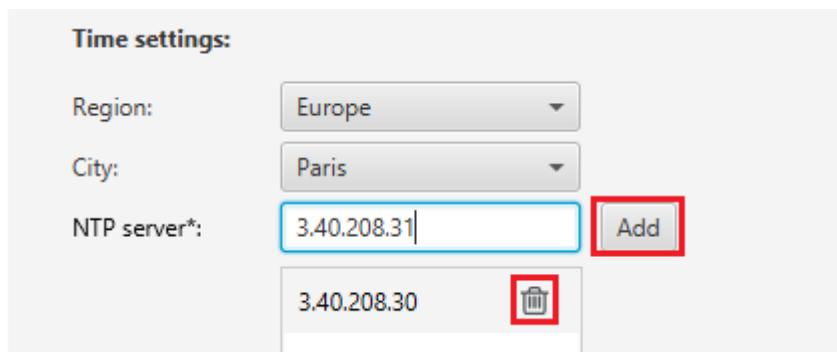
### NOTICE

Using a Time Server is a "MUST" for Scalability. If your virtual AW server is going to be part of a cluster of AW servers, you need to setup a NTP server.

- Click on **Add** to add a NTP server to the list.

### NOTE

Select the  icon to remove a NTP server from the list.



## 2.10.2.5 Configuring the licensing settings

The licenses are generated from GEHC eLicense website with the license ID and the GON (Global Order Number).

- In the **Licenses** tab, click on **Copy** to copy the license ID in the clipboard.

License Name	License Key
AutoBone_Xpress	ZU3C7MOCNJ7N9XS3
Volume_Viewer	3SU9AYMOXVBKNPYX

- Get the site GON (Global Order Number) listed on the site's paperwork from GEHC.

- Generate the eLicenses file:

Refer to [A.3 Licensing on page 556](#) for the complete procedure.

- Click on **Go to eLicense Site** to access the GEHC eLicense website.

- b. Or access the GEHC eLicense website from <http://elicense.gehealthcare.com/elicense/> OR <http://elicense.gehealthcare.com/> - this URL is available via the Internet, and via the GEHC VPN connectivity model.

#### **NOTE**

If you can't connect to eLicense, contact the OLC and ask them to obtain the licensing information for you.

4. Click on the **Browse** button to locate the eLicenses file generated in previous point.
5. Select the eLicenses files then click on **Open** to load the file.

The licenses appear in the *Upload Licenses* list.

## 2.10.2.6 Configuring the platform settings

The Platform Configuration is filled based on the imported eLicense file.

1. In the *Platform Configuration* tab of the Installation Wizard, check the *Platform Integration Mode* information imported from the eLicense file (in [2.10.2.5 Configuring the licensing settings on page 95](#)).

<b>Platform Configuration</b>															
<p>The Platform Configuration is automatically filled based on the imported license file. Please review and select the appropriate configuration and fill out the remaining information if needed. Note : Console Host IP address field is only for Nano licenses.</p>															
<p><b>Platform Integration Mode</b></p> <table border="0"> <tr> <td><input type="radio"/> Standalone</td> <td><input checked="" type="radio"/> Dicom direct connect (PACSSinteg plugin)</td> </tr> <tr> <td>Platform Enabler*:</td> <td>SdC_Low_Tier_Premium</td> </tr> <tr> <td>Platform License Key*:</td> <td>AZXCA27ATFNU2VWN</td> </tr> <tr> <td>Integration License key*:</td> <td>C2TWFYKO7YTODVGC</td> </tr> <tr> <td>Authentication URL:</td> <td><input type="text"/></td> </tr> <tr> <td>Console Host IP address*:</td> <td><input type="text"/></td> </tr> <tr> <td>Preprocessing license key (AutoLaunch)</td> <td>Not set</td> </tr> </table>		<input type="radio"/> Standalone	<input checked="" type="radio"/> Dicom direct connect (PACSSinteg plugin)	Platform Enabler*:	SdC_Low_Tier_Premium	Platform License Key*:	AZXCA27ATFNU2VWN	Integration License key*:	C2TWFYKO7YTODVGC	Authentication URL:	<input type="text"/>	Console Host IP address*:	<input type="text"/>	Preprocessing license key (AutoLaunch)	Not set
<input type="radio"/> Standalone	<input checked="" type="radio"/> Dicom direct connect (PACSSinteg plugin)														
Platform Enabler*:	SdC_Low_Tier_Premium														
Platform License Key*:	AZXCA27ATFNU2VWN														
Integration License key*:	C2TWFYKO7YTODVGC														
Authentication URL:	<input type="text"/>														
Console Host IP address*:	<input type="text"/>														
Preprocessing license key (AutoLaunch)	Not set														

2. Enter the **Authentication URL** only if the PACS/VNA front-end client integration is used.  
Refer to the PACS/VNA/DICOM Remote Host documentation.

## 2.10.2.7 Configuring the license server(s) settings

1. In case of a built-in license server: AW Server has an internal License Server feature, so it can be used as License Server for Applications. If you have received a license key for the built-in server, the License Server configuration is automatically filled based on the imported elicense file. If applicable to your site, configure the **Secondary License Server IP** address in the **Collaborative Server Configuration** tab of the Installation Wizard.

#### **NOTE**

The Secondary License Server is an External License Server.

## License Server Configuration (CoLa Server)

The License server configuration is automatically filled based on the imported license file. In case a Cola Server is not part of your license, you can manually fill the parameters and define external Cola Server. Please review the appropriate configuration.

Built-in

Server enabler: 2DBVD8NGPE8G8OV8

Primary license server IP\*: 127.0.0.1 ✓

Secondary license server IP:

Server port\*: 17767 ✓

2. In case the License Server is not part of the eLicense file, configure the external License Server(s) in the **Cola Server Configuration** tab of the Installation Wizard:

### NOTE

External License Servers are recommended when the site has several devices using Floating License. If it is an AW Server alone, then it is recommended to use the internal (built-in) License Server.

- a. Uncheck the **Built-in** check box.
- b. Enter the **Primary License Server IP** address.
- c. Enter the **Server Port** number: **17767**
- d. If applicable, enter the **Secondary License Server IP** address.

### NOTE

The Secondary License Server can be either the AW Server internal License Server (built-in) or an external License Server. The Second License Server shall only be configured if your site has purchased the CoLA High Availability option.

Built-in

Server enabler: 2DBVD8NGPE8G8OV8

Primary license server IP\*: 3.249.70.232 ✓

Secondary license server IP: 3.249.70.233 ✓

Server port\*: 17767 ✓

## 2.10.2.8 Configuring DICOM hosts

The following procedure describes how to configure one or more DICOM hosts to allow data exchange between them and the AW Server.

1. Get the DICOM hosts information from the IT Admin.
2. Enter the (first) DICOM host information in the **DICOM Hosts** tab of the Installation Wizard. See the example below:

**DICOM host configuration:**

Please fill the information below about your DICOM host configuration.  
Use the "Create host" button to create your DICOM Hosts and continue with the configuration.

**Create new DICOM host:**

Name*:	<input type="text"/>
Host name*:	<input type="text"/>
Application Entity Title*:	<input type="text"/>
IP address or domain name*:	<input type="text"/>
Port*:	4006 <span style="color: green;">✓</span>
Query/retrieve supported:	<input checked="" type="checkbox"/>
Custom search:	<input type="checkbox"/>
Encrypted (TLS)	<input type="checkbox"/>

**Created DICOM hosts:**

toto	<span style="color: green;">✓</span>
------	--------------------------------------

**Create host**

**PACS query retrieve options**

Allow query:   
Allow retrieve:   
Allow store:

**Web Services link option and comments**

Comments:   
Authentication URL:

**Dicom Direct Connect settings**

Preferred compression format: AUTOMATIC  
Allow speed-up of C-FIND query: Multi-value UIDs for C-FIND  
Allow early response for C-STORE:

3. If applicable, check the **Encrypted (TLS)** checkbox to exchange data in secure mode. In this case the certificates shall be exchanged between the AW Server and the DICOM Host. Refer to [2.18.11 Certificate Management on page 211](#).

The **Port** field populates with TLS port number 2762.

#### NOTE

In this case the AW Server DICOM port used to exchange data becomes the port 2762 (default port is 4006). Thus, the AW Server declaration on DICOM images sources should also use the port 2762.

4. If you didn't check **Encrypted (TLS)**, set the **Port** to:
  - **4006** for AW Server DICOM
  - **104** for Universal Viewer and Enterprise Archive DICOM
5. Check **Custom Search** to enable this option and prevent the PQCS/VNQ from querying the whole database. Otherwise, the query may fail due to the high amount of data.
6. **NOTE**

The C-FIND tags are used when NUEVO sends C-FIND commands to the remote host in order to build the Remote Worklist in NoInteg, Hybrid or DDC integration mode. Check or uncheck the box(es) to enable or disable the two optional DICOM tags: **Institution** and **Reading Physician**.

#### NOTE

By default, they are disabled, because, according the IHE standard, remote hosts are not "required" to support them, but many host do (e.g. EA, AWS).

The other C-FIND tags cannot be changed from Service Tools, because, according the IHE standard, remote hosts are "required" to support them. However, if it is really necessary, they can be changed to `false` in the appropriate section in the `network-cfg.xml` configuration file. This configuration file is located in `/export/home/sdc/nuevo/resources/network/network-cfg.xml`. Every DICOM host has a "node" tag structure in the configuration file.

7. To enable the PACS/VNA supporting Storage Commitment:
  - a. Check the **Storage Commitment Supported** option.
  - b. Fill out the **SC host name**, **SC AE title**, **SC IP address** and **SC port**.
8. Check the following options to enable them:
  - **Allow query**: allows the remote DICOM host to query the AW Server
  - **Allow retrieve**: allows the remote DICOM host to retrieve from the AW Server
  - **Allow store**: allows the remote DICOM host to store to the AW Server
9. If applicable, add **Comments** for the FE or IT Admin.
10. In case of front-end integration in DDC or Hybrid mode, enter the **Authentication URL** to authenticate token-based login.
11. In case of DICOM Direct Connect integration:
  - a. Check which compression mode the PACS/VNA supports and select one of the following **Preferred compression format**:
    - **Automatic** (default)
    - **JPEG Lossless**
    - **JPEG 2000 Lossless only**
    - **RLE**
    - **Uncompressed**

- b. Check if the PACS/VNA supports **Relational C-FIND** or **Multi-value C-FIND** and select one of the following in the **Allow speed-up of C-FIND query** field:
- **Relational C-FIND**
  - **Multi-values UIDs for C-FIND** (default)
  - **None**
- c. If applicable, check the **Allow early response for C-STORE** option.  
Checking this option speeds up retrieval of images.
12. Click on **Create host** to complete the host configuration.
13. Repeat previous steps for the next DICOM host configuration.
14. To edit a DICOM host:
- a. Click on the  icon next to the DICOM host name in the list of DICOM hosts.
  - b. Update the DICOM hosts information as described above.
  - c. Click on the **Save** button below the list of DICOM hosts.

## 2.10.2.9 Filling out the device information

All site information must be available for remote use and for other system tools to query.

1. Get the device information from the site IT Admin.
2. Enter the site information in the **Device Info** tab of the Installation Wizard:

See example below:

**Device Information**

Add device information

AWS System ID/AWS CRM number*:	AWBUCLAB243	✓
Contract number:		
Global order number*:	32434534	✓
Install date*:	10/18/2022	 
Expiration date:		 
Device description:		
Hospital name*:	AW BUC ENG LAB243	✓
Address (line 1)*:	Buc	✓
Address (line 2):		
City*:	Buc	✓
State:		
Postal code:		
Country:	FR, France	▼
Other country:		
Address description:		
Service area:		
Service processor IP address:		

3. Enter one of the following in the **Service area** field:
- **APAC for Asia / Pacific**

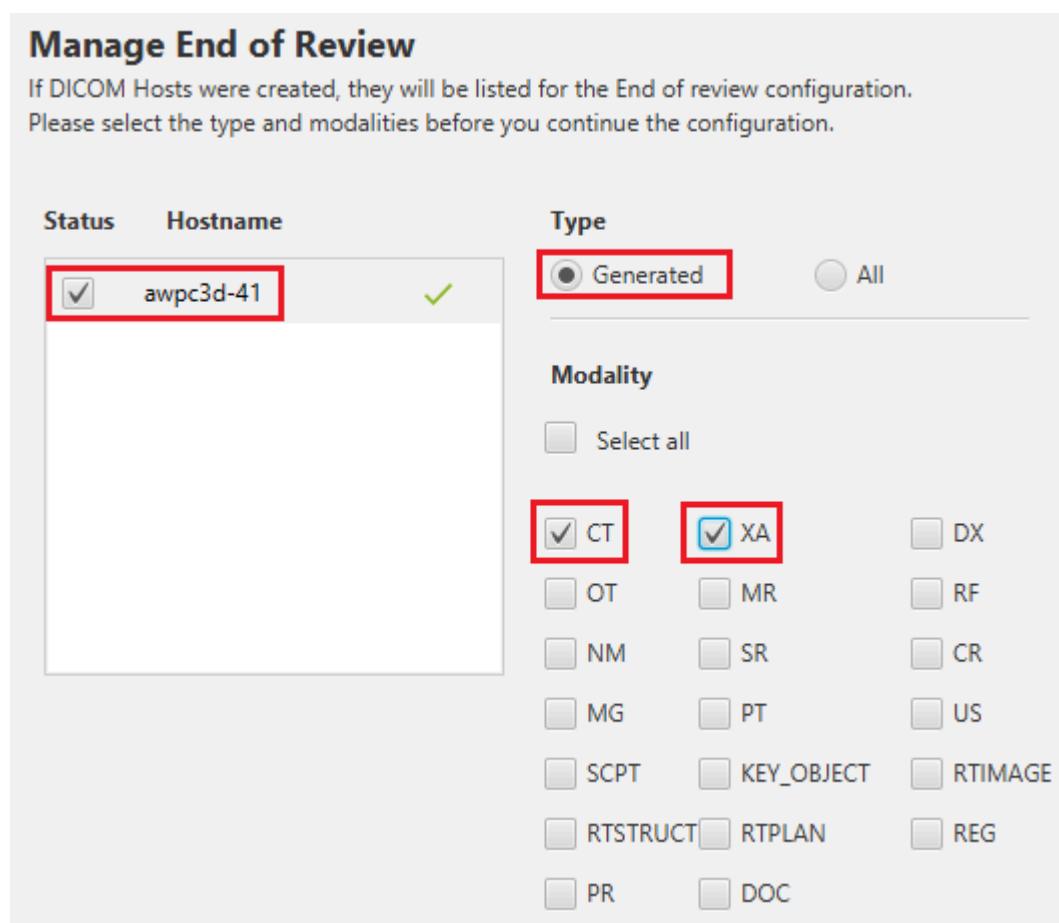
- EU for Europe
- LA for Latin America
- CH for China
- IN for India
- USCAN for US / Canada
- EAGM for Eastern & Africa

## 2.10.2.10 Configuring End of Review

This tab is used to configure "End of Review" processes. When enabled, the End Of Review feature automatically sends processed images to a DICOM host when exiting the application (at tab closure). It is configurable to send which image: "all" or "generated".

After completing a processing procedure, when the Users exit from the feature, they are prompted to choose whether you want to end review. If you choose yes, the AW Server automatically forwards the processed series to any DICOM host connected to the server.

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.



1. In the **End of Review** tab of the Installation Wizard, check the checkbox next to the appropriate DICOM host in the list to enable the End of Review process.
2. In the *Type* panel, select one of the following series to send to the network host after exiting an application:
  - **Generated**
  - **All**

3. In the *Modality* panel, check **Select all** or any combination of modality to send automatically.
4. Repeat the above steps for any other DICOM host(s).
5. To edit an End of Review process for a DICOM host, select the DICOM host in the list of DICOM hosts and update the information as described above.

**NOTE**

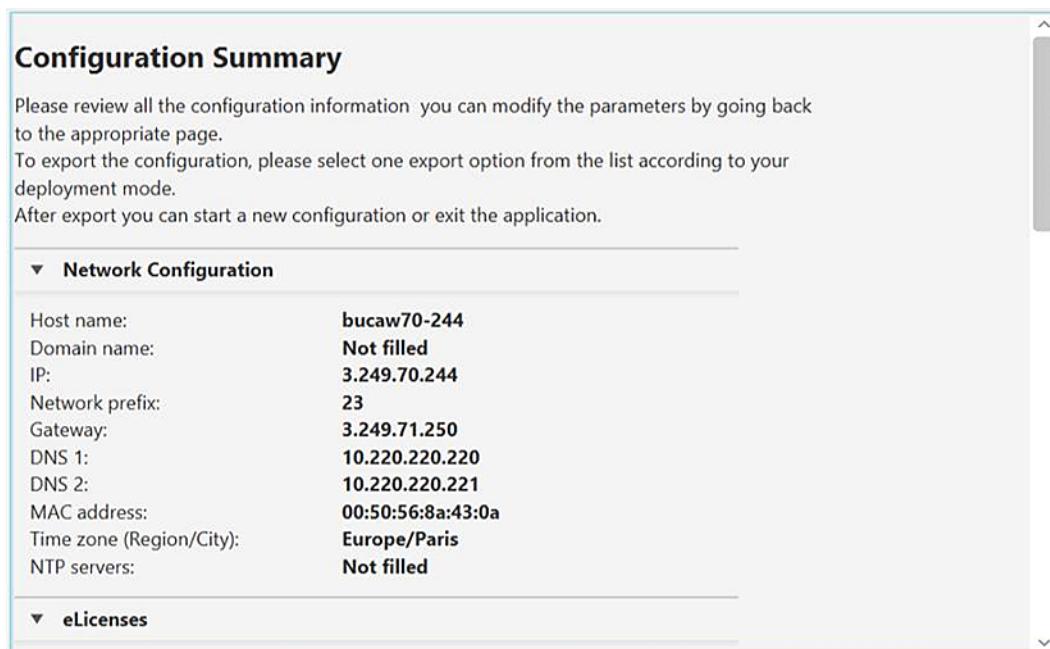
The check next to the **End of Review** tab does not become green as for the other tabs when the End Of Review feature is enabled for DICOM host(s).

**NOTE**

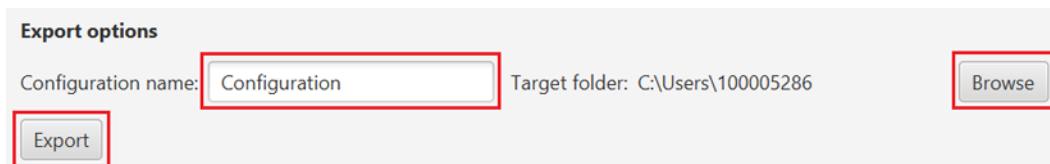
When the End Of Review configuration is changed, the change does not become instantly effective for users that are logged-in, but will become effective starting from the next login session.

## 2.10.2.11 Saving the configuration

1. In the **Summary** tab of the Installation Wizard, review the configuration.  
Use the scroll bar to review the whole configuration.



2. In the *Export options* panel, enter the name of the configuration folder, in which the configuration will be saved, in the **Configuration name** field.
3. Click on **Browse** to choose the location of the configuration folder on your PC.
4. Click on **Export**.



A pop-up appears.

5. Click on one of the following:
  - **Exit** to save the configuration and exit the Installation Wizard,
  - **Start New** to save the configuration and start a new configuration.

The following files are created in the configuration folder (assuming that the name of the folder is **Configuration**)

- **Configuration.iso**: This file is a metafile containing the AW Server Virtual Machine instance information and the configuration data (a yaml file corresponding to the **Configuration.yaml** file). It is attached to the AW Server Virtual Machine during the AW Server configuration.
- **Configuration.yaml**: This file is the configuration file. It contains the AW Server configuration.

**NOTE**

Ignore the other files present in the configuration folder.

**NOTE**

The **Configuration.yaml** file can be kept and reused as a template when configuring the next node in a cluster.

## 2.10.3 Perform the AW Server configuration

This section describes how to configure automatically the AW Server from the configuration iso file (created in previous section: [2.10.2 Preparing the AW Server configuration on page 90](#)) during its first start.

The steps are done at the Client PC.

The configuration iso file will be attached to the AW Server VM as a virtual CD/DVD drive.

While booting up the VM instance, Cloud-init will detect the configuration data, parse and execute its content and effectively configure the AW Server.

After the configuration is done, Cloud-init will be disabled. It can be reenabled from the Service Tools.

1. If the VM is already started, allow the Cloud-init mechanism by typing the following command in a terminal:

**/root/provisioning/cicaws.py enable <Enter>**

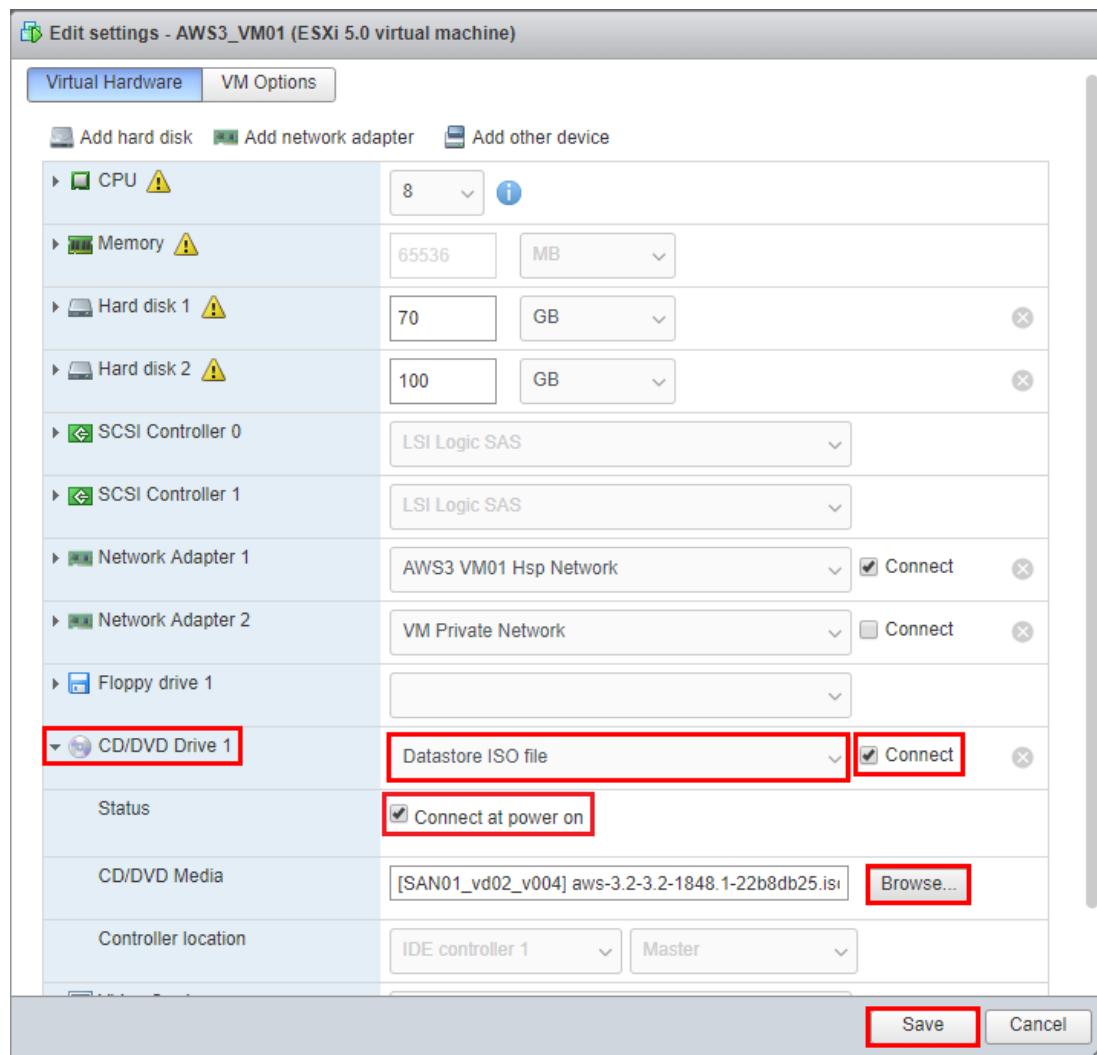
2. Connect to the *ESXi Web Interface*. In the *ESXi Web Interface* login screen (<https://<ESXi URL or IP>/>), login as **service**.

The *ESXi Web Interface* page displays.

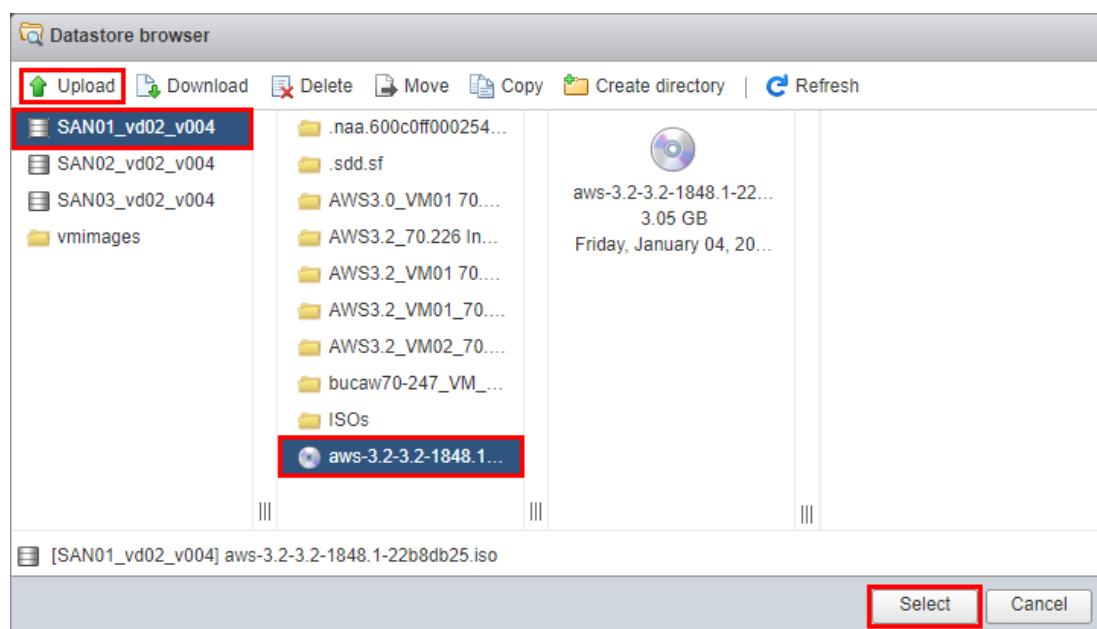
3. Map the iso file containing the user data to the virtual CD/DVD drive:

- Select your Virtual Machine, then click on the  **Edit** icon.

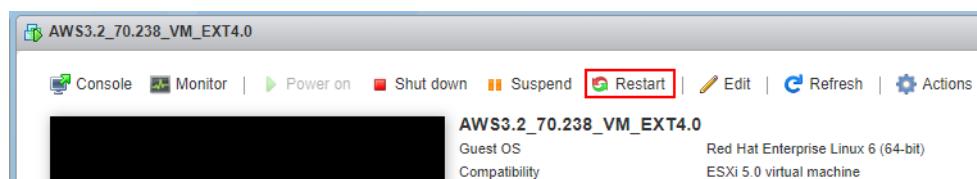
The *Edit settings* screen displays.



- In the **Virtual Hardware** tab select **CD/DVD Drive 1** (or the corresponding name for your VM) from the list.
- If not already selected, select **Datastore ISO file** from the dropdown list. Otherwise, click on the **Browse...** button.
- In the screen that displays:

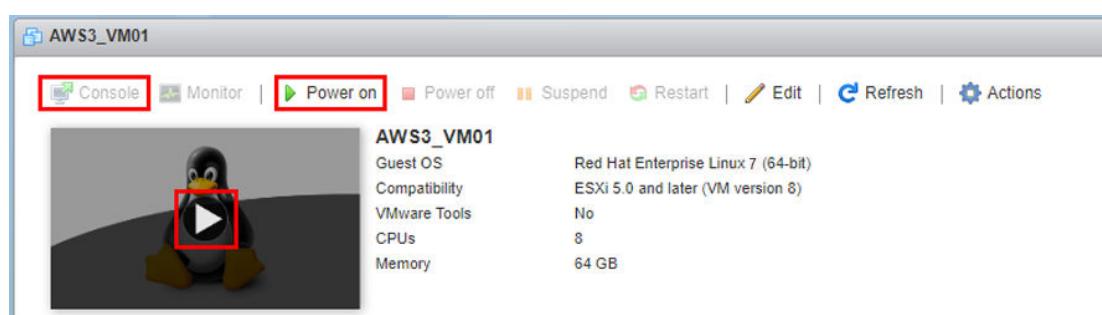


- If the iso file is not already uploaded:
    - Select the datastore where you want to copy the iso file and click on **Upload**.
    - Locate the iso file and select it, then select **Open**.
    - Once uploaded, select the iso file and click on **Select** button.
    - In the *Edit settings* screen check the **Connect at power on** and the **Connect** radio buttons.
    - Click on **Save** button.
4. If the VM is already started:
- a. Restart it by clicking on the **Restart** button.



- b. Proceed to [Step 6](#).
5. If the Virtual Machine is not already started, start the Virtual Machine:
- Click on the Console screen shot (here the white arrow if the Virtual Machine is not already started).

The virtual AW Server OS starts booting up (if not already started) and the Virtual Machine Console opens.



#### NOTE

Once the virtual machine is started, you can also display the Virtual Machine Console by clicking on **Console > Open browser console** or directly on the Console screen shot.

#### NOTE

To work with the Virtual Machine Console, simply click into the console field.

If the screen is black or locked press **<Ctrl>**.

To display the boot sequence while booting press **<Ctrl>** and **<->** simultaneously.

6. Verify the disk partitioning:

- When the boot sequence has completed, click into the console field and login as **root**.
- Verify the partitionning after the OS load. Note that the "Used" and "Available" values may differ from those displayed in the example below:

**df -k <Enter>**

```
[root@bucaw70-243 ~]# df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
/devtmpfs        12304004      0 12304004  0% /dev
tmpfs           12344112      4 12344108  1% /dev/shm
tmpfs           12344112  192640 12151472  2% /run
tmpfs           12344112      0 12344112  0% /sys/fs/cgroup
/dev/sda4       115465340 31957388 77619596 30% /
/dev/sdb1        3778616   15952 3551004 1% /export/backup
/dev/sda1       72248648 11336848 57241784 17% /mnt/HDD_AWEDIMPART
/dev/sda2       20511312   896540 18549812 5% /var/log
/dev/sdb2       1052910236 246568 999155572 1% /export/home1
tmpfs           2468824      0 2468824  0% /run/user/1111
tmpfs           2468824      0 2468824  0% /run/user/0
[root@bucaw70-243 ~]#
```

**NOTE**

For an integrated Virtual AW Server, there is no image data disk (no image filesystem: /export/home1).

**NOTE**

Alternatively, you can use the **df -h** command for display in GBytes

7. Disconnect the iso file from the CD/DVD virtual drive:

- Select the Virtual Machine, then click on the  icon.
- The Edit settings screen displays.
- In the *Virtual Hardware* tab, in front of **CD/DVD Drive 1** (or the corresponding name for your VM) uncheck the **Connect** radio button.
- Click on the **Save** button.
- The following message displays:

"The guest operating system has locked the CD-ROM door..."

Select the **Yes** check box then click on the **Answer** button.

This completes the AW Server configuration with Installation Wizard.

Proceed to [2.14 Job Card IST007 - Service Tools Login on page 131](#).

## 2.10.4 Reenable the Cloud-init mechanism

This section describes how to reenable the Cloud-init mechanism in order to reconfigure automatically the AW Server, from the configuration file, during a next system reboot.

1. If needed, update the configuration file for your AW Server:

The steps below are fully described in section [2.10.2 Preparing the AW Server configuration on page 90](#).

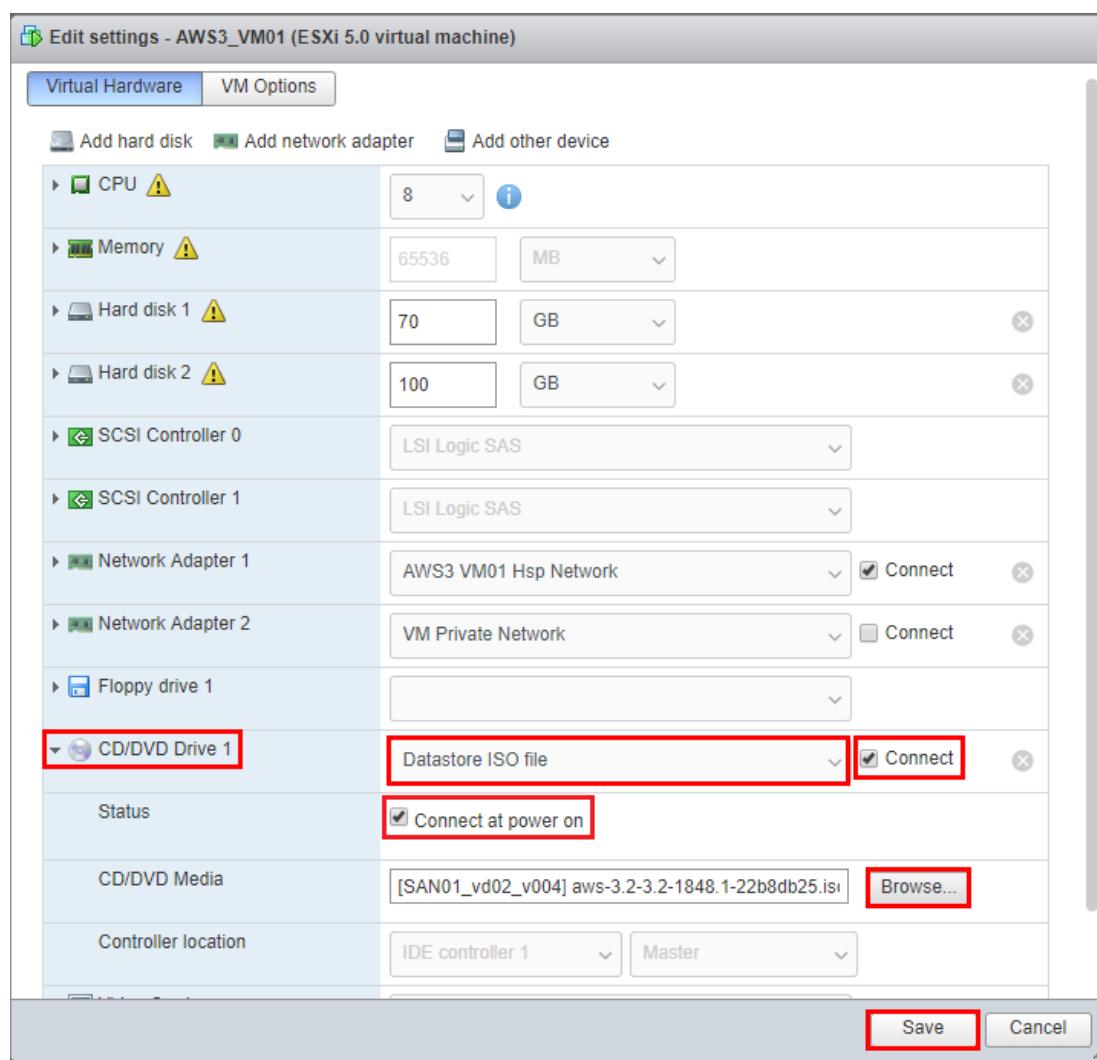
- Launch the Installation Wizard.
  - In the **Start New Configuration** tab, select the **Full configuration** check box and load the configuration file.
  - Update the configuration and save it.
2. Connect to the *ESXi Web Interface*. In the *ESXi Web Interface* login screen (<https://<ESXi URL or IP>/>), login as **service**.

The *ESXi Web Interface* page displays.

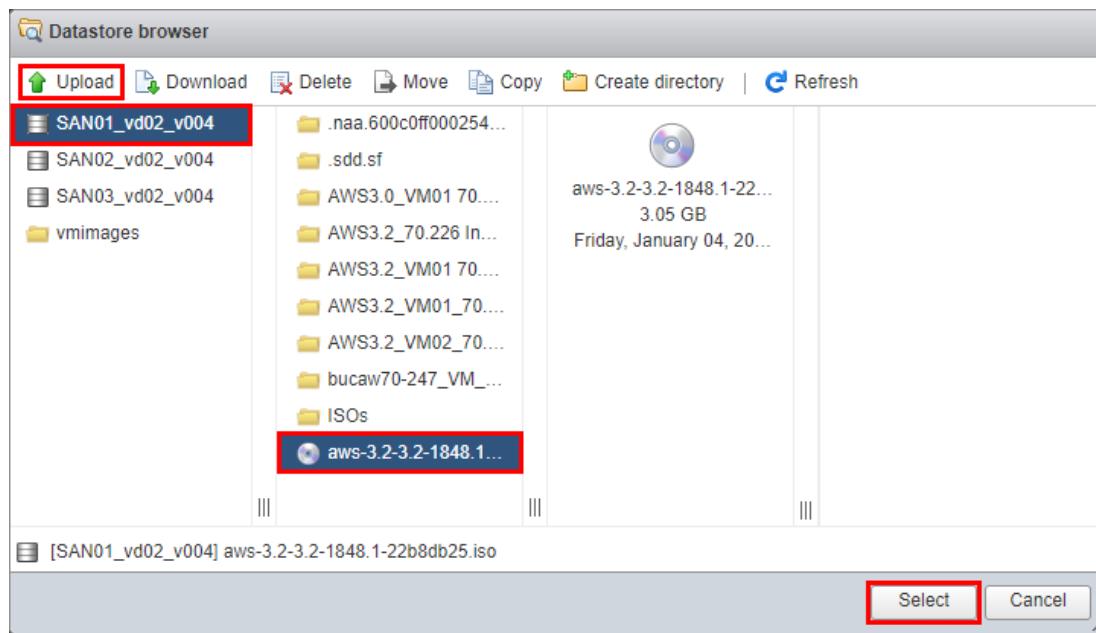
3. Map the configuration iso file to the virtual CD/DVD drive:

- Select your Virtual Machine, then click on the  icon.

The *Edit settings* screen displays.



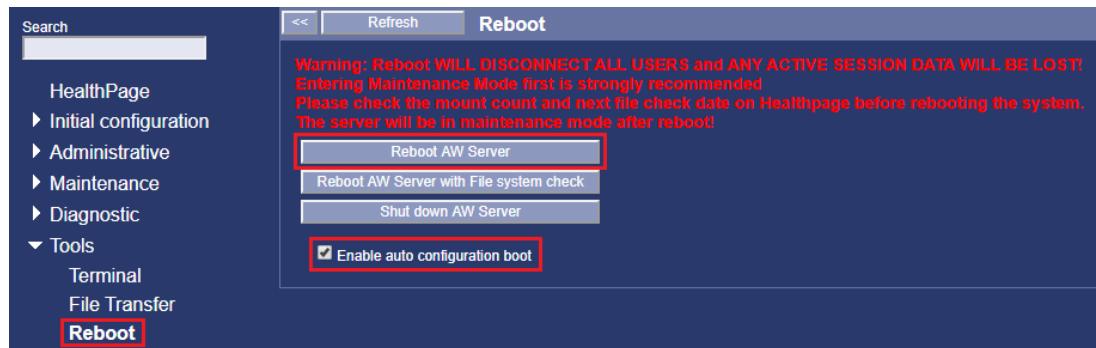
- In the *Virtual Hardware* tab select **CD/DVD Drive 1** (or the corresponding name for your VM) from the list.
- If not already selected, select **Datastore ISO file** from the dropdown list. Otherwise, click on the **Browse...** button.
- In the screen that displays:



- If the iso file is not already uploaded:
  - Select the datastore where you want to copy the iso file and click on **Upload**.
  - Locate the iso file and select it, then select **Open**.
  - Once uploaded, select the iso file and click on **Select** button.
- In the *Edit settings* screen check the **Connect at power on** and the **Connect** radio buttons.
- Click on **Save** button.

#### 4. Reenable the Cloud-Init mechanism:

- In the Service Tools select **Tools > Reboot**.



- Check the **Enable auto configuration boot** check box.
- During the next system reboot the AW Server will be reconfigured from the configuration file.

You can also reboot now by clicking on the **Reboot AW Server** button.

#### 5. Disconnect the configuration iso file from the CD/DVD virtual drive:

##### **NOTE**

After a system reboot, follow the below steps to disconnect the configuration iso file from the CD/DVD virtual drive This will avoid having the AW Server configuration reset after each reboot:

- Select the Virtual Machine, then click on the **Edit** icon.

The Edit settings screen displays.

- In the *Virtual Hardware* tab, in front of **CD/DVD Drive 1** (or the corresponding name for your VM) uncheck the **Connect** radio button.
- Click on the **Save** button.
- The following message displays:

"The guest operating system has locked the CD-ROM door..."

Select the **Yes** check box then click on the **Answer** button.

This completes the AW Server reconfiguration using the Cloud-init mechanism.

## 2.11 Job Card IST003 - Installation of Platform Software

### 2.11.1 AWS Platform software load preparation

The AW Server software is delivered either:

- In the [Physical Software Kit on page 23](#). Use the following file:

Part Number	Content	Purpose	AWS Type	Integration Mode
5872674-6 (or higher)	 aws-3.2-4.9-0.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> . It contains the AW Server software.	Virtual Physical	No-integ Hybrid Seamless DDC

#### NOTE

The reference checksum file (.sha256 extension) is not listed in the table. However, it is present in the USB media to verify file integrity.

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use the following file to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	AWS Type	Integration Mode
5873503-5_AW_Server_3.2_Ext.4.9_Software_and_Docs.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> . It contains the AW Server software.	Virtual Physical	No-integ Hybrid Seamless DDC

#### NOTE

The reference checksum, to verify file integrity, is listed in the *packagemetadata.json* file.

#### NOTE

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

#### 2.11.1.1 Physical AW servers

The steps are done at the Client PC, through the iLO service processor. Refer to [A.6 Software Loading Through iLO on page 579](#).

#### 2.11.1.2 Virtual AW Server

The steps are done at the Client PC.

**NOTE**

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

Map the AWS Platform ISO file from the AWS Platform media to the virtual CD/DVD drive and display the Virtual Machine Console.

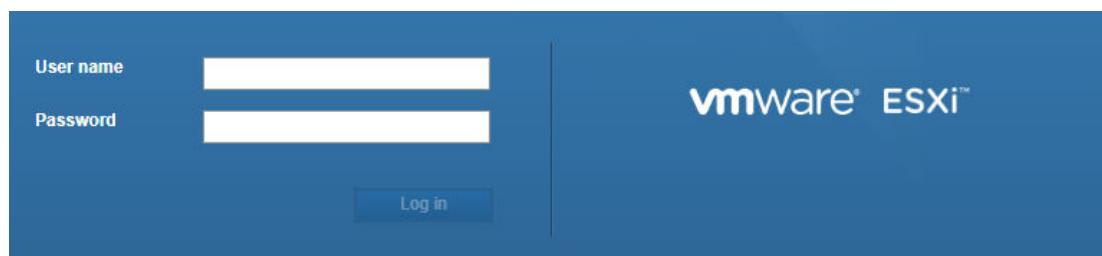
1. Insert the USB media into the Client PC.

2. Connect to the ESXi Web Interface:

- Open a Web browser and enter the URL or IP address of the ESXi:

<https://<ESXi URL or IP>>

The ESXi Web Interface login screen displays:



- Login as **service**.

The ESXi Web Interface page displays.

3. Display the list of Virtual Machines:

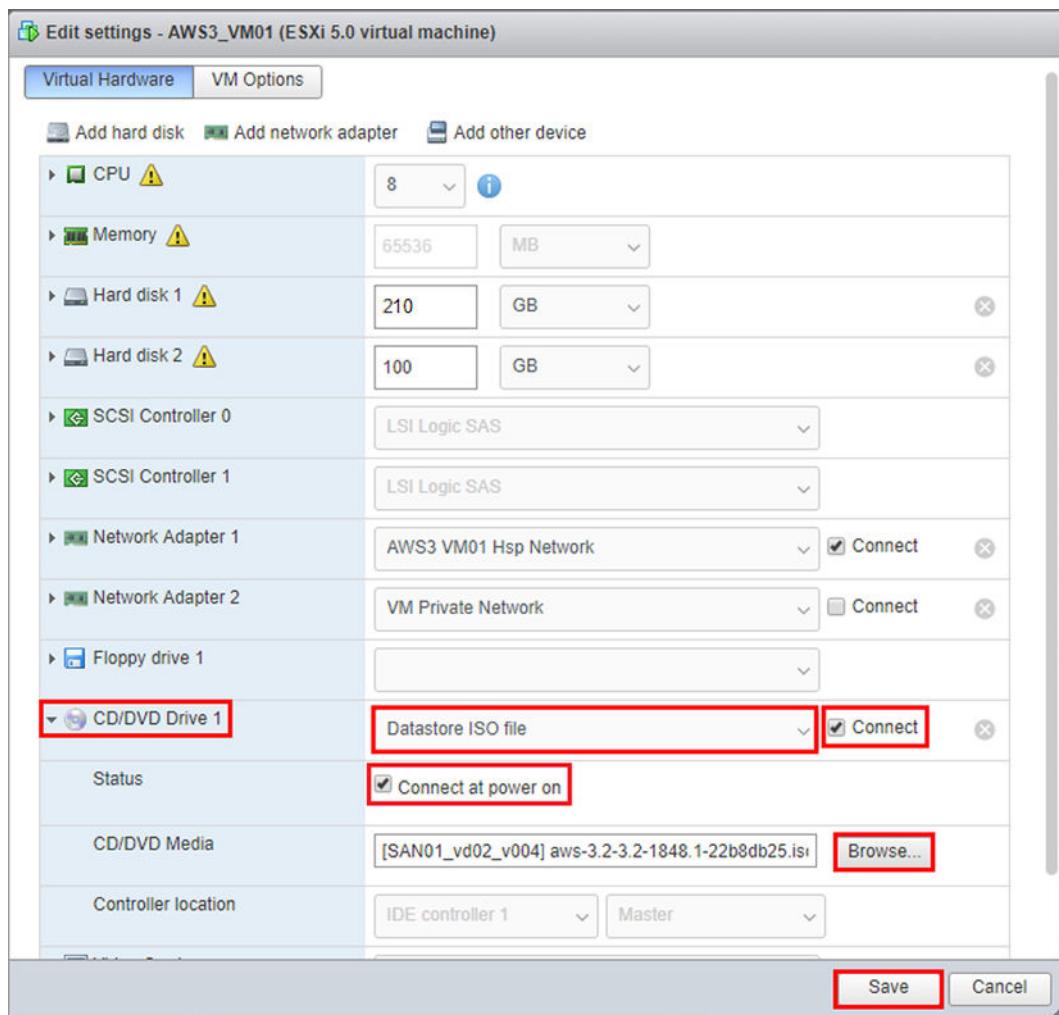
Click on **Virtual Machines** on the left side of the page.

The list of Virtual Machines displays on the right side of the page.

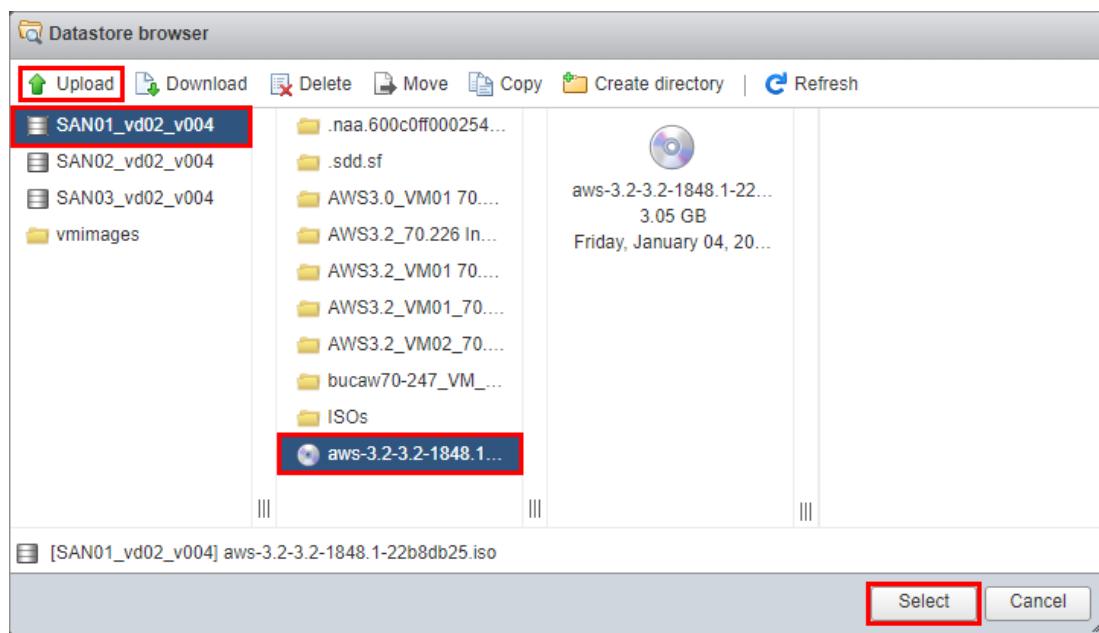
4. Map the iso file to the virtual CD/DVD drive from the Virtual Machine Console:

- Select your Virtual Machine, then click on the  icon.

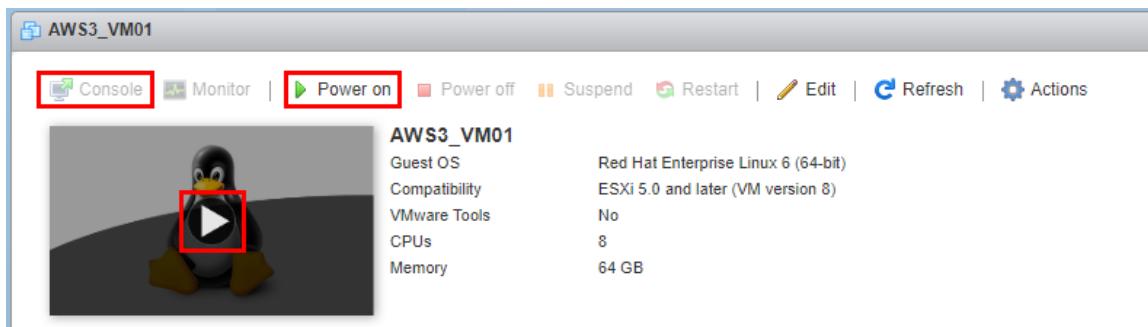
The *Edit settings* screen displays.



- b. In the **Virtual Hardware** tab select **CD/DVD Drive 1** (or the corresponding name for your VM) from the list.
- c. If not already selected, select **Datastore ISO file** from the dropdown list. Otherwise, click on the **Browse** button.
- d. In the screen that displays:



- If the iso file is not already uploaded:
    - Select the datastore where you want to copy the iso file and click on **Upload**.
    - Browse to the USB device of the Client PC. Select the iso file, then select **Open**.
    - Once uploaded, select the iso file and click on the **Select** button.
- e. In the *Edit settings* screen check the **Connect** radio button.
  - f. Click on **Save** button.
5. Start the Virtual Machine and/or display the *Virtual Machine Console* by clicking on the Console screen shot (here the white arrow if the Virtual Machine is not already started).



The virtual AW Server OS starts booting up (if not already started) and the *Virtual Machine Console* opens.

#### NOTE

When the Virtual Machine is started, you can also display the *Virtual Machine Console* by clicking on **Console > Open browser console** or directly on the **Console** screen shot.

#### NOTE

To work with the *Virtual Machine Console*, simply click into the console field.

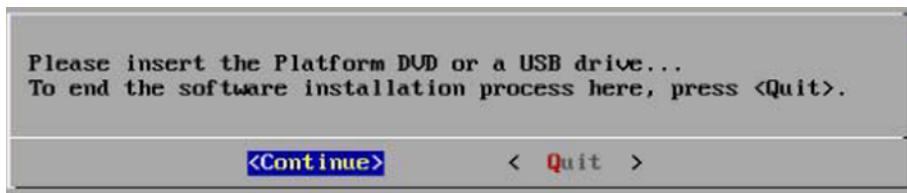
If the screen is black or locked press **<Ctrl1>**.

To display the boot sequence while booting press **<Ctrl1>** and **<->** simultaneously.

## 2.11.2 AWS platform software load

- When the boot sequence has completed, click into the console field and login as **root**.

The following screen pops up:

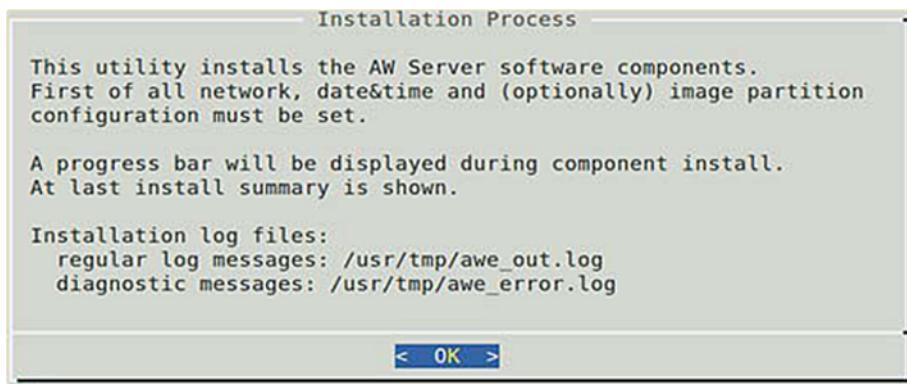


- Mount the platform media:

Press **<Enter>**

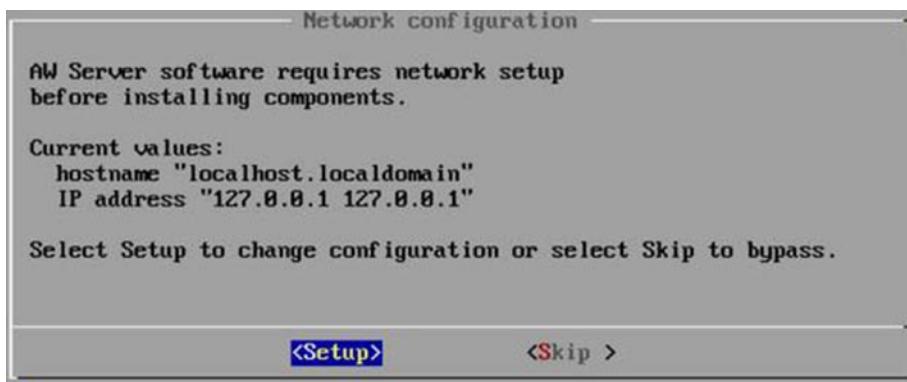
- When the Platform media is mounted successfully a message displays, press **<Enter>** again.

The platform installation utility interface should display, as shown below:



- Press **<Enter>** to continue with the installation.

The following screen displays:

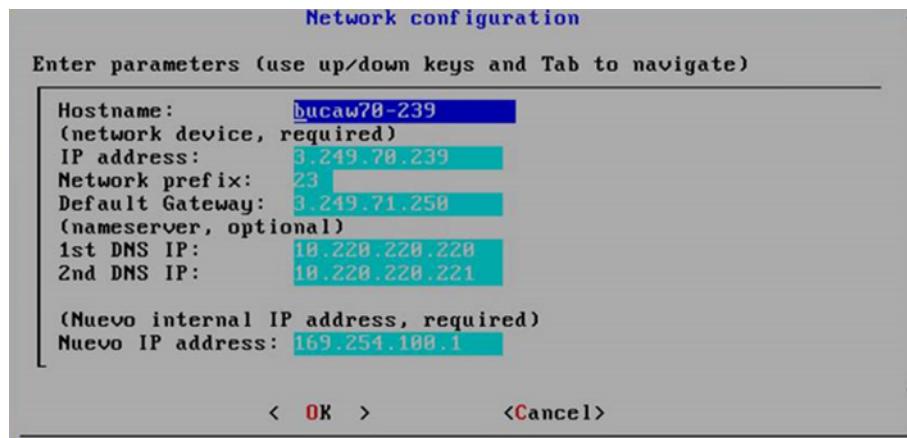


- Network configuration: Obtain all necessary network configuration information from the site IT Admin.

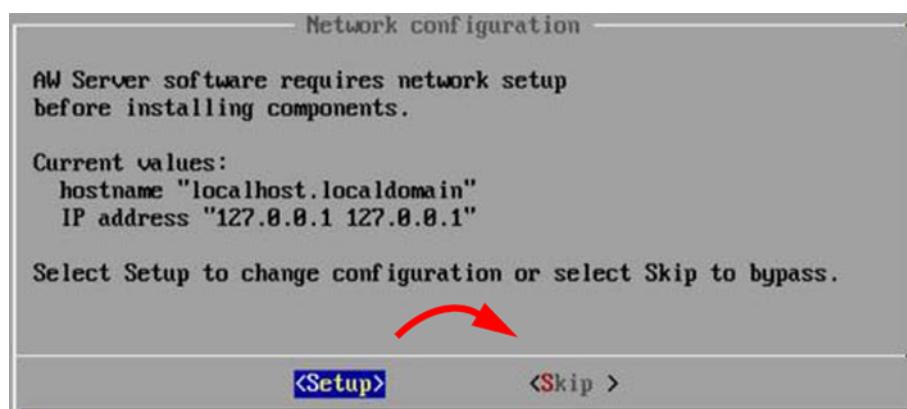
Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

- Keep **<Setup>** selected and press **<Enter>**

- b. Enter the network information in the screen that displays:

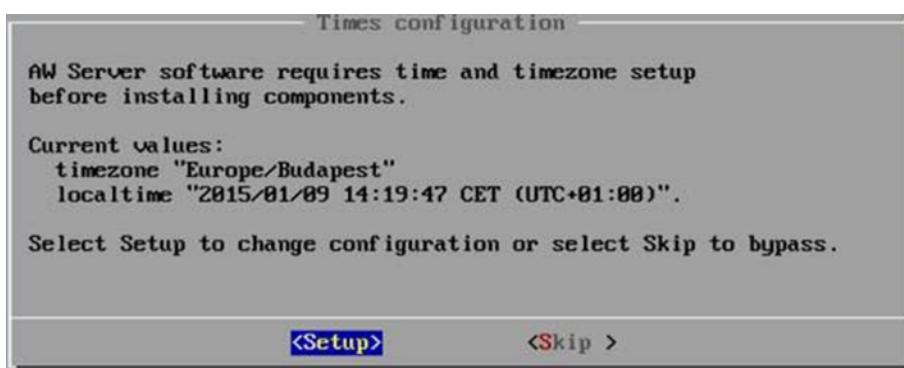


- Enter the Hostname (followed by "dot" Domain\_name if applicable).  
(I.e: **aws-DL560.euro.health.ge.com**)
  - If applicable, enter the parameters for the DNS server(s).
  - Do not touch the Nuevo IP address.
  - When done, tab down to select <OK> and press <Enter> to save the configuration.
- c. The following message pops up again:



If you are done with the Network configuration, now select <Skip> and press <Enter>

## 6. Date and Time Configuration.



- a. Keep <Setup> selected and press <Enter>
- b. Enter the date and time information in the screens that display:
  - Type the number corresponding to the region where your AW Server will be installed, and press <Enter>:

```
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.
#? 2
Select a country (... to skip back)
```

- For instance, after selecting **2** for Americas the following screen displays:

Type the number corresponding to the country where your AW Server will be installed, and press **<Enter>**:

```
10) Pacific Ocean
11) Etc - Specify the time zone using the Posix TZ format.
#? 2
Select a country (... to skip back)
 1) ..          19) Dominica          37) Paraguay
 2) Anguilla     20) Dominican Republic 38) Peru
 3) Antigua & Barbuda 21) Ecuador          39) Puerto Rico
 4) Argentina    22) El Salvador        40) St Barthelemy
 5) Aruba         23) French Guiana      41) St Kitts & Nevis
 6) Bahamas       24) Greenland         42) St Lucia
 7) Barbados      25) Grenada          43) St Maarten (Dutch part)
 8) Belize         26) Guadeloupe        44) St Martin (French part)
 9) Bolivia        27) Guatemala        45) St Pierre & Miquelon
10) Brazil         28) Guyana           46) St Vincent
11) Canada         29) Haiti             47) Suriname
12) Caribbean Netherlands 30) Honduras        48) Trinidad & Tobago
13) Cayman Islands 31) Jamaica          49) Turks & Caicos Is
14) Chile          32) Martinique        50) United States
15) Colombia       33) Mexico            51) Uruguay
16) Costa Rica     34) Montserrat       52) Venezuela
17) Cuba            35) Nicaragua        53) Virgin Islands (UK)
18) Curacao        36) Panama           54) Virgin Islands (US)
#? 1
```

- For instance, after selecting **50** for US the following screen displays:

Type the number corresponding to the Time zone region where your AW Server will be installed, and press **<Enter>**:

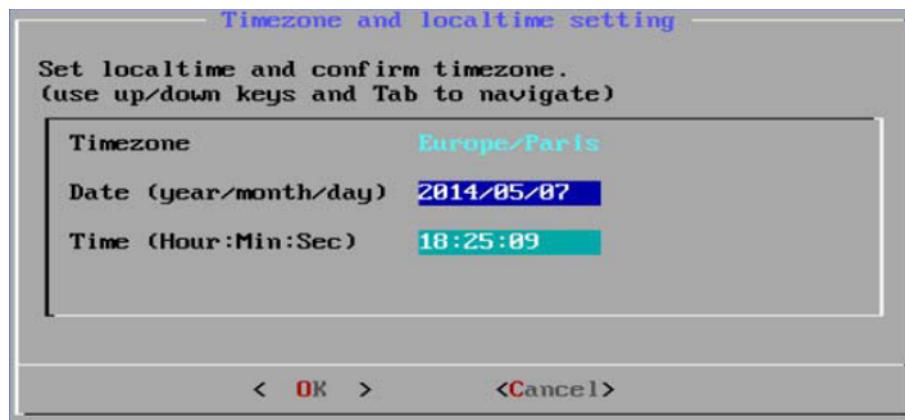
Check with the IT admin of your site what Time zone shall be configured.

```
Select one of the following time zone regions (.. to skip back)
1) ..
2) Eastern Time
3) Eastern Time - Michigan - most locations
4) Eastern Time - Kentucky - Louisville area
5) Eastern Time - Kentucky - Wayne County
6) Eastern Time - Indiana - most locations
7) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
8) Eastern Time - Indiana - Pulaski County
9) Eastern Time - Indiana - Crawford County
10) Eastern Time - Indiana - Pike County
11) Eastern Time - Indiana - Switzerland County
12) Central Time
13) Central Time - Indiana - Perry County
14) Central Time - Indiana - Starke County
15) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
16) Central Time - North Dakota - Oliver County
17) Central Time - North Dakota - Morton County (except Mandan area)
18) Central Time - North Dakota - Mercer County
19) Mountain Time
20) Mountain Time - south Idaho & east Oregon
21) Mountain Standard Time - Arizona (except Navajo)
22) Pacific Time
23) Pacific Standard Time - Annette Island, Alaska
24) Alaska Time
25) Alaska Time - Alaska panhandle
26) Alaska Time - southeast Alaska panhandle
27) Alaska Time - Alaska panhandle neck
28) Alaska Time - west Alaska
29) Aleutian Islands
30) Hawaii
#?
```

### NOTE

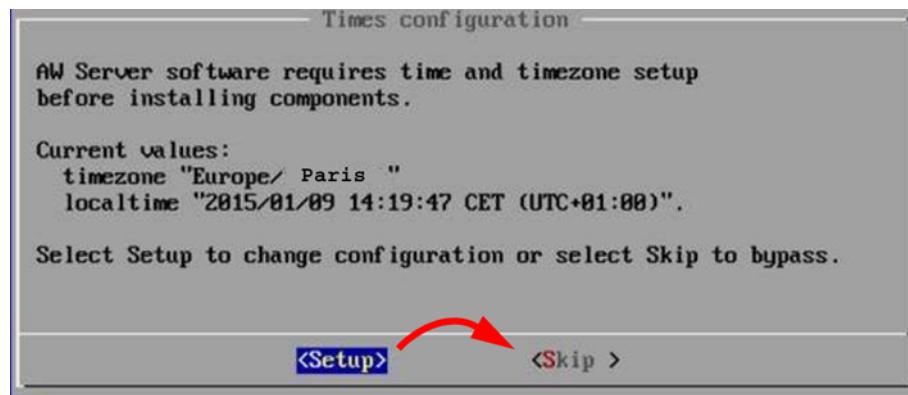
This step is required for countries having several Time zones.

- When done, the following screen will display to let you modify the Date and Time if necessary:



- Check or modify the date accordingly.
- Press arrow down to check or modify the time accordingly.
- When done, tab down to select <OK> and press <Enter> to save the configuration.

- c. The following message pops up again:

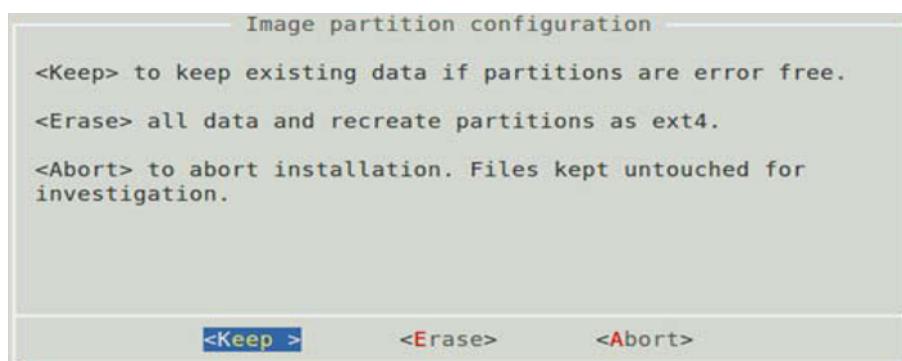


If you are done with the Time zone configuration, now select **<Skip>** and press **<Enter>**

7. When done, the system continues the software loading.

The message **Image partition must be checked** may display briefly.

The *Image partition configuration* screen displays.



8. Image partition configuration:

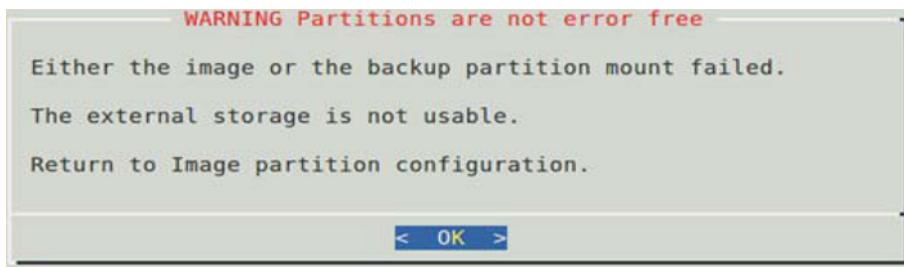
- Select **Keep** and press **<Enter>** to preserve existing images (upgrade / reinstallation case). In this case the image filesystem will be kept as "Ext3" type (upgrade case).
- OR

#### **NOTICE**

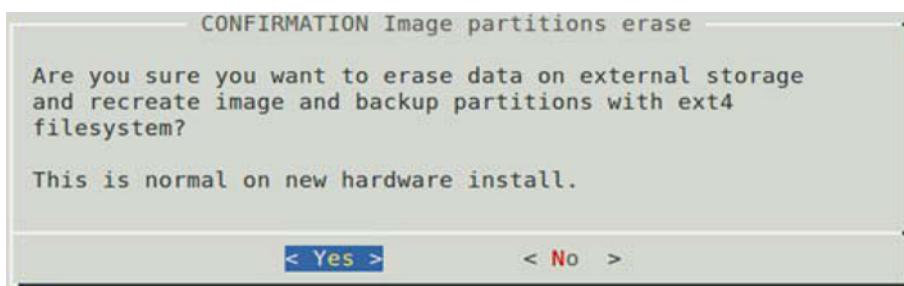
Preferably select **Erase** and press **<Enter>** (new installation case or upgrade / reinstallation case when the customer agrees that existing images can be deleted). In this case the image filesystem will be created as the new "Ext4" type (faster than Ext3 filesystem) ----- **Recommended setting !!!**  
-----

#### **NOTE**

If the following screen displays, it means that there were already some data on the image disks array that cannot be used. In this case, acknowledge the message by selecting **<OK>** and pressing **<Enter>** to return to the previous menu, then choose **Erase** to delete image data from the disks and recreate the partitions.



- If you choose to erase the Image partition, the following confirmation screen displays. Select **Yes** and press **<Enter>** to confirm image partition deletion and re-creation as Ext4 filesystem type.



#### 10. Virtual machines only:

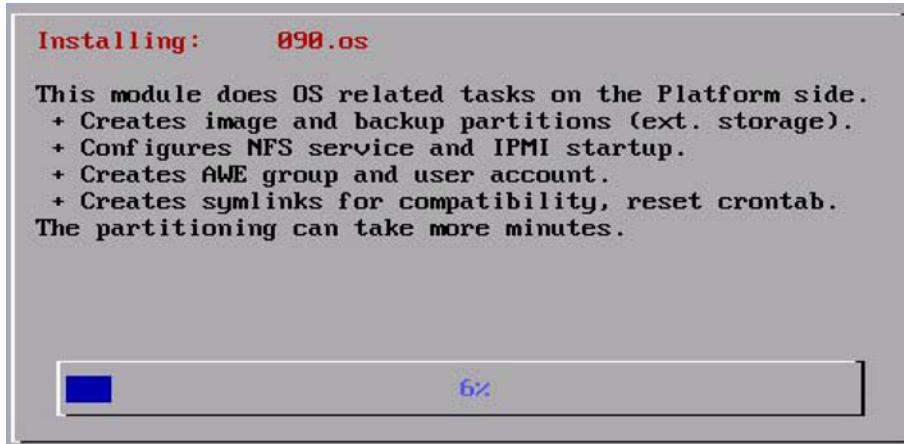
The following menu ONLY SHOWS when you install a virtual machine to let you choose between an AW Server installation or a Preference Storage server.

Highly Available Preference Storage servers (HAPS) are aimed to serve Preferences between the virtual AW servers within a cluster (Scalability).



- To install an AW Server, keep the default selection and press **<Enter>**, then continue with the next installation steps. OR
- To install a HAPS server, select **HAPS** using the keyboard arrow key, then press **<Enter>** and jump to [2.11.3 HAPS Server installation on page 122](#).

- AWS Platform software installation starts. Various progress screens display with self-explanatory status indicators of the installation progress.



#### NOTE

Installation of the 090.os package may take several minutes when the image partition is not empty. Please be patient.

- When all packages are installed, the following message displays:

```
"Installation completed ...
All packages installed with success.
Please press <Enter> to continue"
```

Press **<Enter>** to continue.

- When the load process completes, the *Status Result* box (shown in the following illustration) displays.

Install Summary (all Passed)			
100.java	Passed	700.awe	Passed
150.hardware	Passed	725.icm	Passed
170.hws	Passed	750.service	Passed
200.tomcat	Passed	755.hardening	Passed
220.edisonmachine	Passed	760.psm	Passed
300.security	Passed	770.jumai	Passed
305.rsvp	Passed	785.prodiag	Passed
307.softwaredownload	Passed	799.dotmed	Passed
310.eat	Passed	810.awcomponentregistration	
320.ea3	Passed	820.astp	Passed
330.firewall	Passed	835.aia	Passed
350.cmservice	Passed	840.dicom_streaming	Passed
380.els	Passed	845.mediaviewer	Passed
390.nuevo	Passed	850.ng_media	Passed
395.dtex	Passed	860.config_service	Passed
405.cola	Passed	870.mailsender	Passed
410.colaserver	Passed	880.webaccess	Passed
415.pacsinteg	Passed	899.system_config	Passed
450.modgecsi	Passed	999.postInstall	Passed
			100%
OK			

Use the keyboard arrow keys or the **<Space>** bar to scroll through all the package installation results and verify that all the packages were installed successfully.

- If any package reports as Failed, reload the AWS software as a first step (restart at [Step 1](#)). If it fails again, reload the Operating System (OS), then reload the AWS software.
- After you check all packages are successfully installed, press **<Enter>** to continue.

A EA3 password change window pops up informing that you need to change passwords for the **admin** and **service** users.



16. Press **<Enter>**.

A prompt asks you to type the new password for the **admin** user.



17. Refer to [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for the password change guidelines.

- Enter the new **admin** user password and press **<Enter>** to continue.

A prompt asks you to type again the new password for the admin user.

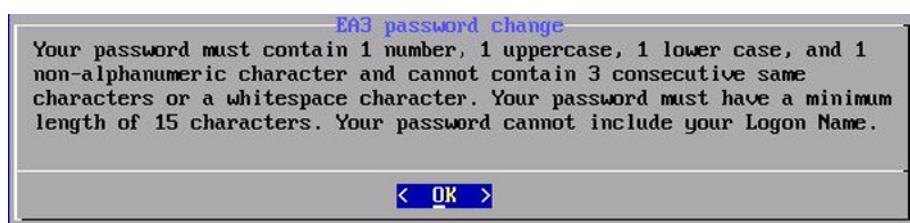


18. Enter again the new **admin** user password and press **<Enter>** to confirm.

If the password is successfully updated, a notification appears.



If the password does not comply with the password policy, the rules display and you have to enter a new password.



19. Repeat the procedure (from [Step 16](#) to [Step 18](#)) for the **service** user.

Unmounting media followed by Installation Completed messages display.

20. Press **<Enter>**.
21. If the system doesn't reboot, type **reboot** and press **<Enter>**.

**NOTE**

Once you have pressed **<Enter>** to exit, YOU CANNOT GO BACK TO SCROLL THROUGH THE RESULTS LIST!

The AW Server reboots.

22. When the AW Server completes the reboot sequence, login as **root**.
23. Check the partitioning of the AW Server. Type the command:

```
df -k <Enter>
[root@bucaw70-243 ~]# df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
devtmpfs        12304004      0  12304004  0% /dev
tmpfs          12344112       4  12344108  1% /dev/shm
tmpfs          12344112  192640 12151472  2% /run
tmpfs          12344112       0  12344112  0% /sys/fs/cgroup
/dev/sda4     115465340 31957388 77619596 30% /
/dev/sdb1      3778616   15952 3551004 1% /export/backup
/dev/sda1     72248648 11336848 57241784 17% /mnt/HDD_AWEDIMPART
/dev/sda2      20511312   896540 18549812 5% /var/log
/dev/sdb2     1052910236  246568 999155572 1% /export/home1
tmpfs          2468824       0  2468824  0% /run/user/1111
tmpfs          2468824       0  2468824  0% /run/user/0
[root@bucaw70-243 ~]#
```

**NOTE**

The **Used** and **Available** values slightly differ from those displayed above, depending on the type of AW Server (Physical or Virtual, Low Tier or High Tier).

**NOTE**

For an integrated Virtual AW Server, there is no image data disk (no image filesystem: `/export/home1`).

24. **Virtual server case only:** Disconnect the iso file from the CD/DVD virtual drive:

- a. Select the Virtual Machine, then click on the  **Edit** icon.

The *Edit settings* screen displays.

- b. In the *Virtual Hardware* tab, in front of **CD/DVD Drive 1** (or the corresponding name for your VM) uncheck the **Connect** radio button.
- c. Click on the **Save** button.

- d. The following message may display:

The guest operating system has locked the CD-ROM door...

Select the **Yes** check box then click on the **Answer** button.

25. **Physical server case only:**

- a. Verify that the iLO and the default gateway have been configured with the site-assigned static IP address designated by the site admin, with the following command:

```
/sbin/hponcfg -w /tmp/asd <Enter>
grep IP /tmp/asd <Enter>
```

I.e: `<IP_ADDRESS VALUE = "3.249.14.205">` This is the iLO IP address.

`<GATEWAY_IP_ADDRESS VALUE = "3.249.15.254">` This is the default gateway IP address.

**NOTE**

If using iLO 3, there is a firmware minor display issue when setting the Default Gateway IP address, as shown above. The Default Gateway IP address can be entered and successfully saved, but when exiting and returning to the setup menu, it will keep on displaying as `0 . 0 . 0 . 0`, even though the entry is properly taken into account by the system.

- b. Check that the Default Gateway IP address has effectively been taken into account by pinging the iLO or connecting to the iLO.
    - Open a command prompt and type: `ping 3.249.14.205 <Enter>`.
    - Open a navigator window and enter: `http://3.249.14.205 <Enter>`
26. Eject the media and store it in a safe place for future use.

**NOTE**

Details of the installation results can be viewed in the Service Tools in **Diagnostic > Log Viewer** or with the following commands in the command prompt:

Command	Result
<code>cat /var/tmp/AweResults.out &lt;Enter&gt;</code>	Synthesized list of results of AWS platform software installation
<code>cat /var/log/gehc/install-stdout.log &lt;Enter&gt;</code>	Detailed list of results of AWS platform software installation
<code>cat /var/log/gehc/install-error.log &lt;Enter&gt;</code>	List of errors during AWS platform software installation

This completes the AWS software load.

- **Physical hardware AW Servers:**

Proceed to [2.12 Job Card IST004A - HPE R/T3000 UPS drivers setup on page 123](#)

- **Virtual AW Servers:**

Proceed to [2.14 Job Card IST007 - Service Tools Login on page 131](#).

- **Virtual HAPS Servers:**

Proceed to [2.11.3 HAPS Server installation on page 122](#)

- **Software upgrade:** Go to the section [3.10.4.4 AW Server Platform software installation on page 517](#) for reference, before proceeding to:

- Physical servers: [2.12 Job Card IST004A - HPE R/T3000 UPS drivers setup on page 123](#)
- Virtual servers: [2.14 Job Card IST007 - Service Tools Login on page 131](#)

## 2.11.3 HAPS Server installation

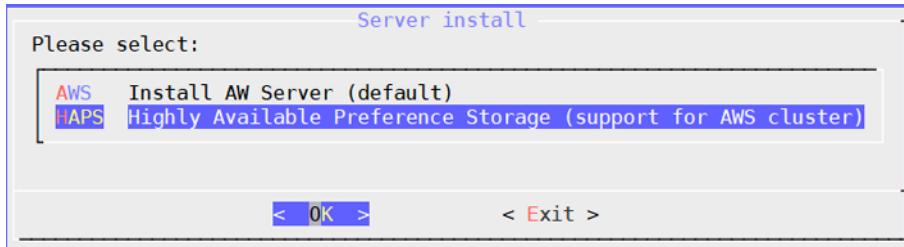
**NOTICE**

The NTP (Network Time Protocol) server must be up and running, prior to install the HAPS servers.

For Virtual AW Servers in a cluster (Scalability), in order to achieve high availability, it is mandatory to setup **two HAPS** (High Availability Preference Sharing) servers.

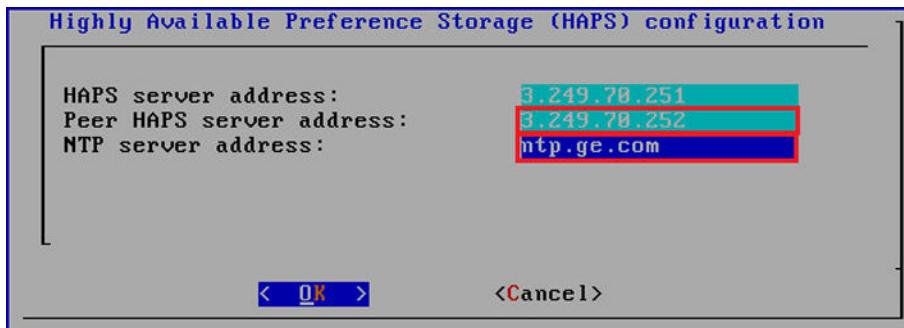
The following steps detail the installation of the HAPS servers.

- At the AW Server / HASP Install choice screen: select:



- Select **HAPS Highly Available Preference Storage (support for AWS cluster)**.
- Select **OK** and press **<Enter>**

- Configure the HAPS server:



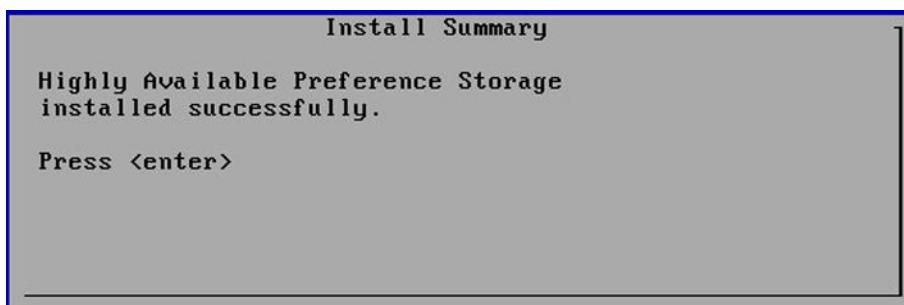
- Enter the peer HAPS server IP address (current HAPS server IP address is prefilled).
- Enter the NTP server IP address.
- Select **OK** and press **<Enter>**

- When all packages have been installed, the following message displays:

```
"Installation completed ...
All packages installed with success.
Please press <Enter> to continue"
```

Press **<Enter>** to continue.

- When installation of the HAPS server has completed, the following message displays:



Press **<Enter>**

This completes the HAPS servers software load.

## 2.12 Job Card IST004A - HPE R/T3000 UPS drivers setup

This section applies to the optional HPE R/T3000 UPS drivers loading on Physical AW Server High Tier (GEHC delivers the hardware). It is not applicable to Virtual AW Server.

**Bypass this step if NO UPS option.**

**NOTICE**

Your new AW Server 3.2 hardware system **has been preloaded** with OS and AWS platform software, and UPS drivers (if applicable) by GEHC Manufacturing.

## 2.12.1 HPE R/T3000 UPS drivers installation verification

The Operating System and the AW Server platform software shall be loaded.

The UPS utility driver is part of the AWS Platform software and is automatically loaded and installed when loading the AWS software from media. Check that the UPS driver has been properly installed on the system.

1. Login as **root**.
2. Type the following:

```
ls -la /usr/local/HP/PowerProtector <Enter>
```

3. Verify that the folder contains the following files and folders:

- bin
- configs
- db
- desktop
- HP-HPPP
- install.log
- mc2

Proceed to configuration. Go to [2.12.2 Configuring the HPE R/T3000 UPS using HPPP Software on page 124](#).

## 2.12.2 Configuring the HPE R/T3000 UPS using HPPP Software

1. Verify that all server equipment options are connected to power ports on the UPS rear panel.
2. Make sure that the USB cable (or Serial) connecting the UPS to the server is properly installed.
3. Launch a supported Internet browser:

Locally at the KVM:

- a. Launch the server's GUI using the command: **startx <Enter>**. Refer to [A.8.7 Launching the Internet Navigator from the Server's KVM on page 591](#), for instructions.
- b. Launch the Firefox Internet browser from the desktop.
- c. In the URL field, enter the address:

```
localhost:4679
```

From a remote host:

- a. Open the Terminal from **Service Tools > Tools** and login as **root**.
- b. Disable the firewall with the command:  

```
systemctl stop pnf <Enter>
```
- c. Open an Internet browser, and in the URL field, enter:  

```
http://<ip_address>:4679 (for a standard connection)
```

or `http://<ip_address>:4680` (for a secure connection)  
 where `<ip_address>` is the IP address of the server hosting HPPP.

4. Close the HP Power Protector Notification window that sticks in the foreground of other windows.
5. Read and accept the HP End User License Agreement (click on the **Accept** button)
6. Log into HP Power Protector (HPPP) using the default credentials user/password.  
 The message You are using the default password ... displays.
7. Click on **OK**.  
 The *HP Power Protector Configuration* screen opens.
8. Select **Administrator** and click on **Save**.



The Main window of HPPP *HP Power Protector - Administrator* opens.



This screen allows an administrator to:

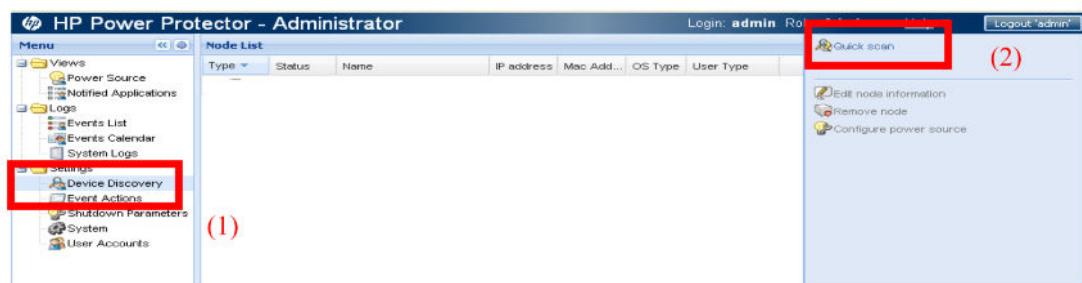
- discover attached UPS's,
  - edit the UPS or application information,
  - configure the power source and redundancy,
  - manage users accounts.
9. Change the **admin** password to increase security:
    - a. Select **Users Accounts** (1).
    - b. Click on the **admin** account (2).
    - c. Click on **Edit user** (3).
    - d. In the popup that displays, enter and confirm the new password.
- Refer to Job Card [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for choosing a secure password.

- e. Click on the **Save** button.

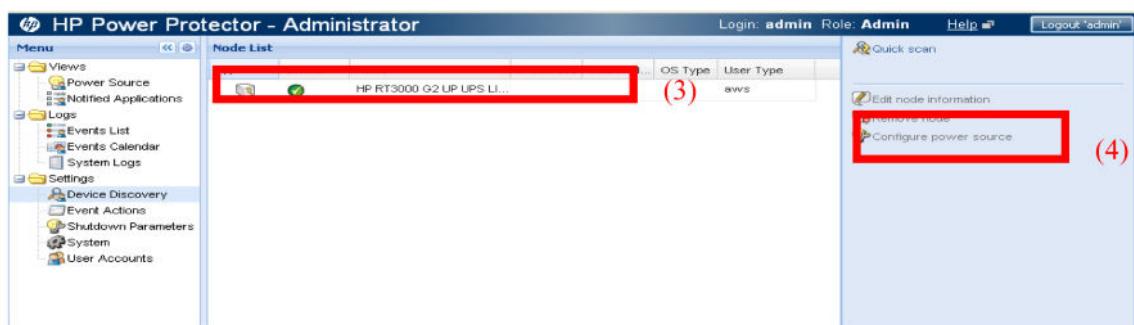


10. Discover the power source on the Device Discovery screen:

- a. Click on **Device Discovery** (1) to display the *Device Discovery* screen. You can use this to identify and connect to UPS's connected to the server via serial and USB.
- b. Click on **Quick scan** (2).

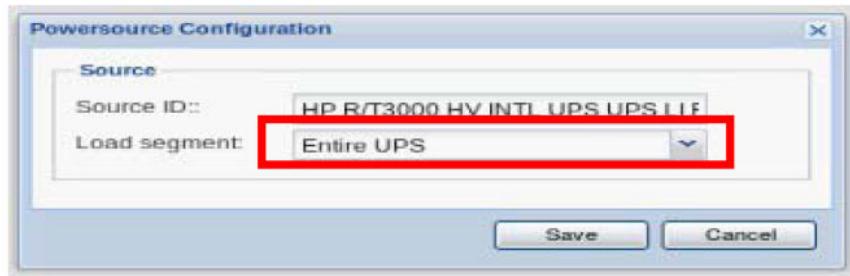


After a moment, the menu displays a list of the UPS found (only one in our case).



11. Select the HPE R/T3000 UPS Device (3).
12. Select the device that powers the server:
  - a. Click on **Configure Power source** (4).

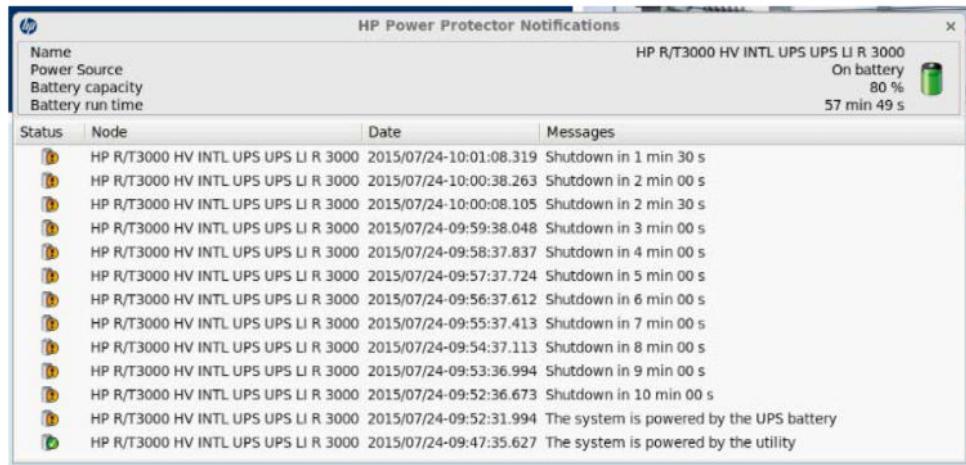
The *Powersource Configuration* screen opens:



- b. Select **Entire UPS** in the pull-down menu of the **Load Segment** field.
- c. Click on **Save**.
- 13. Logout from the *HP Power Protector - Administrator* by clicking on the **Logout 'admin'** button at the upper right of the window and on **Yes** at the confirmation popup message.
- 14. Verify that the UPS auto-shutdown feature is operational:

- a. Power off the UPS (unplug it from the AC Mains supply).

The *HP Power Protector Notifications* window shall pop up and display the time remaining before shutdown. The default delay before starting shutdown is set to 10 minutes.



- b. Verify that the server shuts down after 10 minutes if the AC is not restored before.
- 15. When the shutdown is completed, restore power to the UPS.
- 16. Turn on the AW server and check that the boot up sequence completes normally.
- 17. If you have previously disabled the PNF firewall to allow connection from a remote host, enable it back:

- a. Open the Terminal and login as **root**.
- b. Re-enable the Firewall with the command:

```
iptables -F <Enter>
systemctl start pnf <Enter>
```

The HPE R/T3000 UPS configuration is complete.

**Proceed to 2.21 Job Card IST006 - Changing the Passwords on page 249.**

## 2.13 Job Card IST005 - Network and Time Configuration

## 2.13.1 Network Configuration

### 2.13.1.1 Important information about Hostname

For hostname characters rules and limitations, refer to [A.2 Specific field - Characters rules and limitations on page 555](#).

#### NOTE

If the rules and limitations are not respected, the script `/root/sys-net-conf` doesn't allow to set the hostname. The procedure has to be run again with a correct value for hostname.

- Once the network parameters have been setup, you can see the result by typing:

```
cat /etc/hosts <Enter>
```

Example of `/etc/hosts` file:

```
192.0.4.25 aws-06 aws-06
```

```
or 192.0.4.25 aws-06.euro.health.ge.com aws-06.euro.health.ge.com
```

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.

### 2.13.1.2 Network Configuration Procedure

This section describes how to setup the Network configuration manually.

- Obtain all necessary network configuration information from the site IT Admin.
- Launch the Network configuration tool:

For factory preloaded hardware servers, at boot up time for a factory preloaded AW Server (see [2.5 Job Card IST001A - Hardware Installation Verification on page 45](#)), you can launch it:

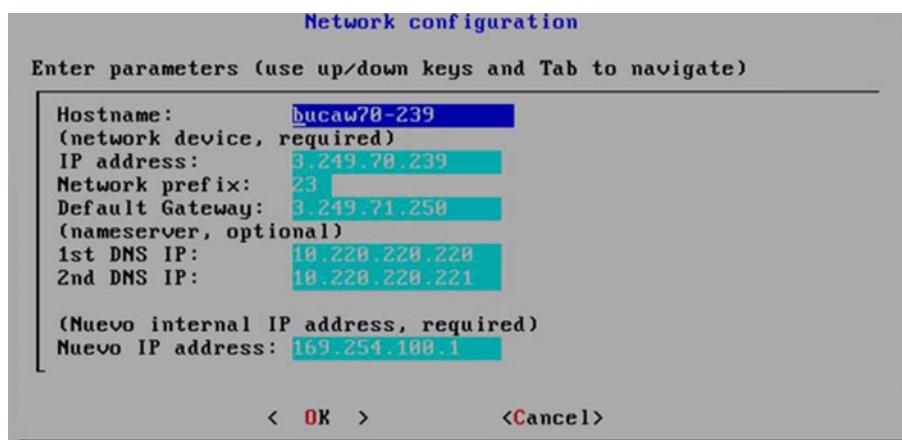
- locally, at the server's KVM.
- remotely, using the iLO service processor and the remote console (see next steps).

For other cases:

- Open a remote console/terminal.
- Login as `root`.
- Type the command:

```
sh /root/sys-net-conf <Enter>
```

The following screen displays:



3. Enter the Hostname (followed by "dot" Domain\_name if applicable).  
(I.e: **aws-DL560.euro.health.ge.com**)
4. If applicable, enter the parameters for the DNS server(s).
5. Do not touch the Nuevo IP address.
6. Tab down to select **<OK>** and press **<Enter>** to save the configuration.
7. If you need to access the Service Tools, reboot the AW Server (see [2.13.3 Reboot the AW Server on page 131](#)).

**NOTE**

You can check the domain name by opening a Terminal and using the commands:

**dnsdomainname** or **hostname -d**.

**NOTICE**

The Network configuration is not part of the backup/restore configuration feature of the Service Tools. Upon installation, record all Network parameters in the Maintenance logbook so you are able to retrieve them in case future reinstallation would be needed. Record parameters for both the AW Server(s) and the HAPS server(s).

The Network configuration is complete.

Proceed to [2.13.2 Date and Time Configuration on page 129](#).

## 2.13.2 Date and Time Configuration

This section describes how to setup the Time zone configuration manually.

1. Launch the Date and Time configuration tool:

For factory preloaded hardware servers, at boot up time for a factory preloaded AW Server (see [2.5 Job Card IST001A - Hardware Installation Verification on page 45](#)), you can launch it:

- locally, at the server's KVM.
- remotely, using the iLO service processor and the remote console (see next steps).

For other cases:

- a. Open a remote console/terminal.

- b. Login as **root**.

- c. Type the command:

**sh /root/sys-times-conf <Enter>**

The following screen displays to let you choose the Time Zone:

```
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.
#? 2
Select a country (... to skip back)
```

2. Type the number corresponding to the region where your AW Server will be installed and press **<Enter>**.

For instance, after selecting **2** for Americas the following screen displays:

```
#, Indian Ocean
10) Pacific Ocean
11) Etc - Specify the time zone using the Posix TZ format.
#? 2
Select a country (... to skip back)
 1) ..          19) Dominica          37) Paraguay
 2) Anguilla    20) Dominican Republic 38) Peru
 3) Antigua & Barbuda 21) Ecuador          39) Puerto Rico
 4) Argentina   22) El Salvador        40) St Barthelemy
 5) Aruba       23) French Guiana      41) St Kitts & Nevis
 6) Bahamas     24) Greenland         42) St Lucia
 7) Barbados    25) Grenada          43) St Maarten (Dutch part)
 8) Belize      26) Guadeloupe        44) St Martin (French part)
 9) Bolivia     27) Guatemala         45) St Pierre & Miquelon
10) Brazil      28) Guyana           46) St Vincent
11) Canada      29) Haiti            47) Suriname
12) Caribbean Netherlands 30) Honduras        48) Trinidad & Tobago
13) Cayman Islands 31) Jamaica          49) Turks & Caicos Is
14) Chile       32) Martinique        50) United States
15) Colombia    33) Mexico           51) Uruguay
16) Costa Rica   34)Montserrat       52) Venezuela
17) Cuba        35) Nicaragua         53) Virgin Islands (UK)
18) Curacao    36) Panama           54) Virgin Islands (US)
#? 
```

3. Type the number corresponding to the country where your AW Server will be installed and press **<Enter>**.

For instance, after selecting **50** for US the following screen displays:

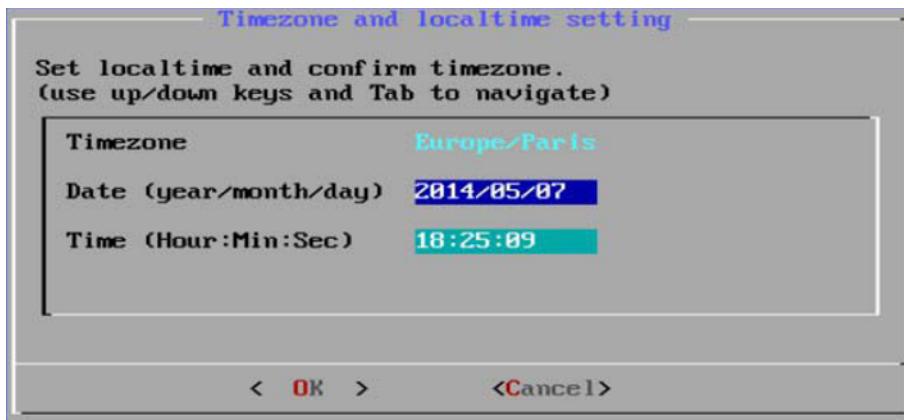
```
Select one of the following time zone regions (... to skip back)
 1) ..
 2) Eastern Time
 3) Eastern Time - Michigan - most locations
 4) Eastern Time - Kentucky - Louisville area
 5) Eastern Time - Kentucky - Wayne County
 6) Eastern Time - Indiana - most locations
 7) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 8) Eastern Time - Indiana - Pulaski County
 9) Eastern Time - Indiana - Crawford County
10) Eastern Time - Indiana - Pike County
11) Eastern Time - Indiana - Switzerland County
12) Central Time
13) Central Time - Indiana - Perry County
14) Central Time - Indiana - Starke County
15) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
16) Central Time - North Dakota - Oliver County
17) Central Time - North Dakota - Morton County (except Mandan area)
18) Central Time - North Dakota - Mercer County
19) Mountain Time
20) Mountain Time - south Idaho & east Oregon
21) Mountain Standard Time - Arizona (except Navajo)
22) Pacific Time
23) Pacific Standard Time - Annette Island, Alaska
24) Alaska Time
25) Alaska Time - Alaska panhandle
26) Alaska Time - southeast Alaska panhandle
27) Alaska Time - Alaska panhandle neck
28) Alaska Time - west Alaska
29) Aleutian Islands
30) Hawaii
#? 
```

#### 4. **NOTE**

This step is required for countries having several Time zones.

Check with the IT admin of your site what Time zone shall be configured (where your AW Server will be installed) and type the number corresponding to the Time zone region, and press **<Enter>**.

The following screen displays:



5. Check the **Date** and **Time** fields and, if necessary, modify them.
6. Tab down to select **<OK>** and press **<Enter>** to save the configuration.
7. If you need to access the Service Tools, reboot the AW Server (see [2.13.3 Reboot the AW Server on page 131](#)).
8. **NOTICE**

If your site has NTP server(s), you must configure it (them). This is a mandatory step if your AW Server is going to be part of a cluster of virtual AW server systems.

Configure NTP Time server(s) with the Service Tools interface (refer to [2.15.6.2 Time Server menu on page 149](#)).

## 2.13.3 Reboot the AW Server

### NOTICE

After any configuration or configuration change of the Network parameters and/or the Date & Time parameters, it is necessary to reboot the AW Server. If the AW Server is not rebooted after network configuration change, the Service Tools cannot be accessed.

To reboot the server, proceed as follows:

1. Make sure you are still logged as **root** or login as **root**.
2. Type in the reboot command:  
**reboot <Enter>**
3. Wait for boot completion before proceeding to the next setup steps.

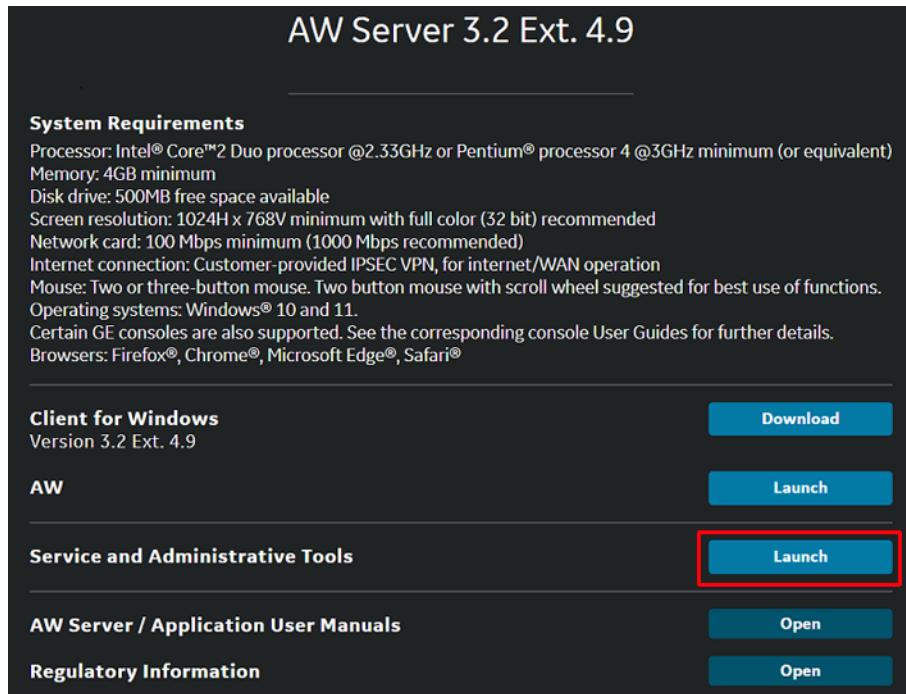
## 2.14 Job Card IST007 - Service Tools Login

The following Configuration steps shall be done from the Client PC, or from the FE laptop connected and configured for the Hospital network. In case none of them is available at this time, the Internet navigator can be launched at the KVM. See [A.8 Useful Commands and Tools on page 589](#).

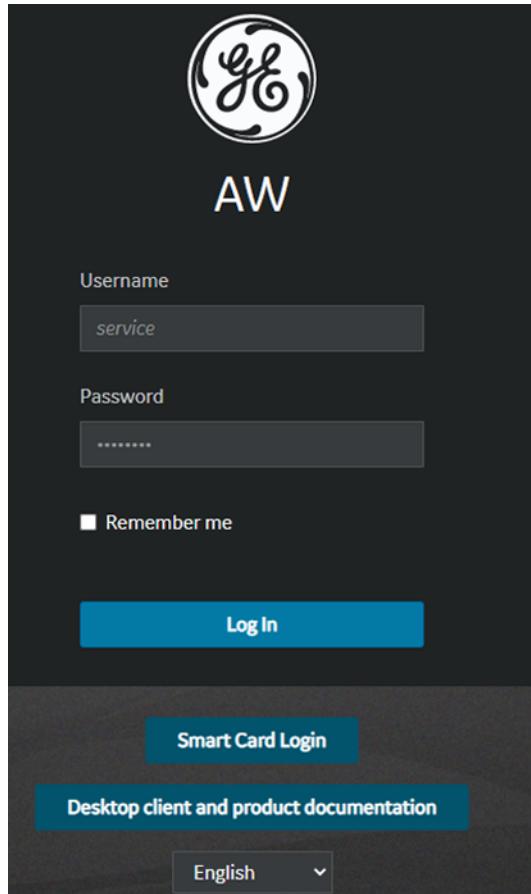
### 2.14.1 Logging into Service Tools

1. At the Client PC or FE laptop, open a browser (refer to [1.6 Supported Web Browsers on page 27](#)) and type in the AW Server's IP address : `http://<server_IP_address>`
2. Accept the cookies in the window that popups.

- When the page loads, click on the Service and Administrative Tools **Launch** button shown in the following illustration.



- The login screen appears.



## 5. Login as **service**.

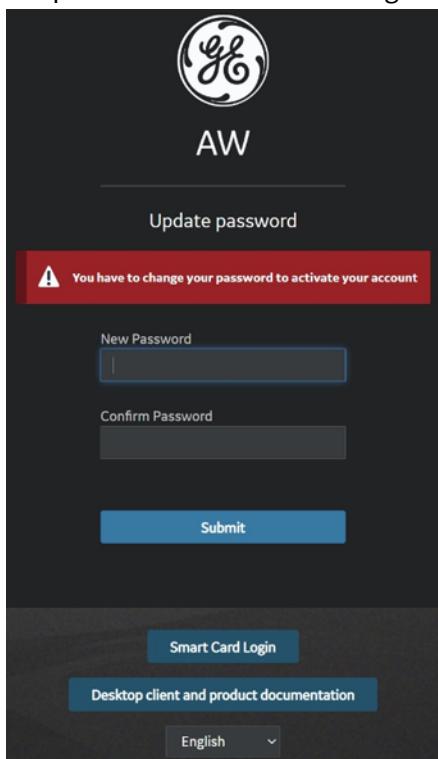
### NOTE

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

### NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for the password change guidelines.

The Service Tools *HealthPage* appears.

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

### NOTE

If the AW Server has been configured automatically with the Installation Wizard and the Cloud-init mechanism, the configuration status in the Healthpage takes several minutes (around 3 to 5 minutes) to display after the login prompt appeared. This delay occurs at the first login into Service Tools. Use the **Refresh** button to refresh the HealthPage.

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

## 2.14.2 HealthPage Examples

The following examples show the different sections of the HealthPage displayed for the HP High Tier server, the HP Low Tier server, and for the Virtual server.

The HealthPage also displays the "license ID" of your AW server, necessary to calculate the licenses corresponding to the "GON" for the site from the eLicense Internet site at:

<http://elicense.gehealthcare.com/>

It is important to make sure that the Hardware subsystems status, as well as the Memory and Disks status DO NOT display in RED, that would mean reporting an error condition.

**NOTE**

Display in Yellow can have two different meanings: Warning or information not available. For the HP Low Tier and HP High Tier servers, the Fan, Power, UPS status and Voltage information may not be fully available, so this information will not be displayed in green but in yellow. However, when any of these device fails, status will display in RED.

### 2.14.2.1 HealthPage Status example- HP server

Fan, Voltage and Power status can display in "Yellow" for HP servers, in normal working conditions.

Hardware Subsystem	Status
Temperature	OK
Fan Status	OK
Voltage	Not applicable
Power Status	OK
UPS Status	Not applicable
RAID Status	OK

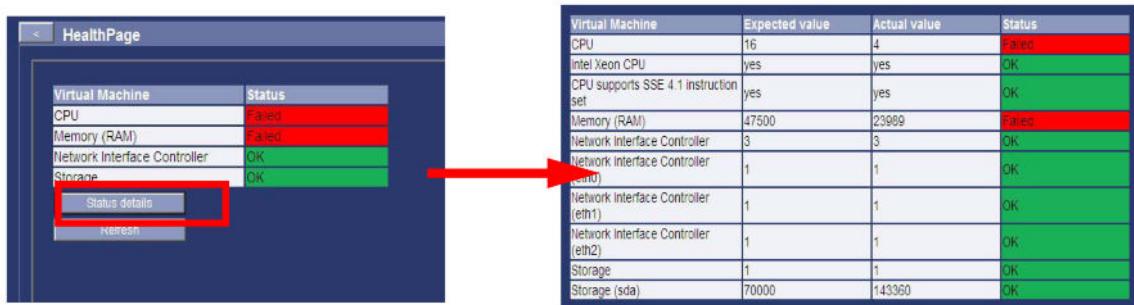
### 2.14.2.2 HealthPage "Status" example- Virtual server

In a Virtual environment, all Status shall display in green provided that the appropriate resources have been setup on the physical server, for hosting the Virtual AW Server.

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

In case some of the status would display in red, as in the following example, contact the IT Admin of the site to fix the issue and get the appropriate physical resources granted to your Virtual AW Server.

- Click on **Status details** button for more information on the issue.



#### NOTE

After the upgrade of a Seamless Integrated AW Server, the storage temporarily appears as failed in Healthpage, until the configuration (seamless integration) has been restored.

### 2.14.2.3 HealthPage "System Configuration" example

The following example shows the System configuration status page for an AW Server before complete setup. Therefore, the Registration status shows as Invalid and displays in red. As long as the registration status is not complete, the AW Server is not able to quit the Maintenance mode.

System Configuration	
System ID (CRM Number)	AWBULCLAB239
Platform version	aws-3.2-4.4-2140.4-28fd1663
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239
Encrypted (TLS) AET / Port	bucaw70-239 / 2762
Plain AET / Port	bucaw70-239 / N/A
CPU (8)	Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9
Modality OS Version	AWS3.2 OS 7.0 [20210902]
UDI	(01)00840682102384(10)AWS03D02E4D4
REF	5719780
LOT	AWS03D02E4D4
Uptime	12 days
Region / Timezone	Europe / Paris
Memory Total / Free	98304 (MB) / 88011 (MB)
OS Disk Space Total / Free	110 (GB) / 91 (GB)
Image Disk Space Total / Free	110 (GB) / 76 (GB)
Backup Disk Space Total / Free	110 (GB) / 91 (GB)
Log Disk Space Total / Free	19 (GB) / 18 (GB)
Network Queue Status	In progress: 0 Pending: 0 Paused: 0 Failed: 0
Auto Delete (High / Low)	-
Delete option for worklist browser	Off
Image partition mount count (Current / Max.)	Not applicable
Image partition next file system check date	Not applicable
Signer certificate expiration date	Mon 25 Oct 2027 11:45:19 AM CEST
Certificate expiration date	Mon 28 Nov 2022 10:45:19 AM CET
AW Access certificates expiration date	N/A
Clam AV Antivirus Software status	Not activated
Machine type	VMware Virtual Platform ESXi
Install mode	server
DICOM AET (printing)	PR_bucaw70-239
Service Processor	N/A
License ID	068adb65
Integration	DICOM Direct Connect
Cluster mode	False
Registration status	Invalid
Registration key	InvalidKey
Automatic Configuration Status Summary	N/A
Secured for RMF	Off
RMF activation date	N/A
RMF verification date	N/A

### 2.14.2.4 HealthPage "Remote Service" example

The following example shows the connectivity status.

Here the RSvP remote service has been configured and the RSvP Agent is connected to the back office. So, the system is ready to be accessed remotely.

#### NOTE

When the *RSvP Status* is **Unused** with blank background, the RSvP Agent is not running. For any other statuses, the RSvP Agent is running with issue or not completely configured.

IRIS is running, meaning that the automatic loading of new package (eg: new applications versions, ...) is available using RSvP connectivity.

Remote Service	
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
IRIS Next Execution	Wed 16 Jun 2021 03:11:30 AM CEST
<input type="button" value="Refresh"/>	

#### 2.14.2.5 HealthPage "Version Information" example

The following example shows the version of the different "SW components" running on the AW server.

Version Information	
EC-Workspace	1.0.9
EC-Navigator	1.0.4
EC-Worklist	1.0.7
EC-Preview Pane	1.0.6
EC-Dicom Web Service	1.0.0
EC-XE Service	1.0.0
IF-Imaging Fabric	1.4.2
IF-Setup Operator	1.4.2
EML-Central Configuration Store	1.0.8
EML-Certificate Management Service	3.2.0
EML-Filewatcher Service	3.2.0
EML-Centralized Logging Service	1.0.1
EML-Security Auditing Service	3.2.0
EML-Postgres Service	1.7.0
EML-Messaging Service	1.7.0
EML-Docker	19.03.11
EML-Helm	3.2.4
EML-Kubernetes	1.20.1
Component Registration	1.0.3-1
AWS build date	20210720
AWS version	aws-3.2-4.2-2129.2-c8bbb739
EA3	ea3-4.9-2.11_RFV_V2_EA3.noarch
EAT	eat-2.4-2.11_RFV_V2_EAT.noarch
Nuevo	nuevo-CSERelease_4_21-RFV1_V4_NUEVO.x86_64
CoLA	cola-3-3.x86_64
Service Tools	ServiceTools-3.2.4.2-c8bbb739.noarch
Service Tools AWS	ServiceTools_AWS-3.2.4.2-c8bbb739.noarch
Dotmed	dotmed-2.5.5-CSERelease_4_21_RFV1_V4_DOTMED.x86_64
AIA	6.0-16.46
Filmer	6.0-16.46
ICM	icm-4.4.9-1.noarch
RSvP	2.3
IRIS	2.3.0-2
ELS	1.3.0-1
<input type="button" value="Refresh"/>	

#### 2.14.2.6 HealthPage "Configuration & Status" display

To display or pull from system the Configuration page, click on the **Display** or **Pull from system** buttons.



It will take a few moments for the system to gather the information and either display the configuration information into an additional window (click on the **Hide** button when done to close the window), or to propose downloading the configuration into a Zip file.

The result displayed by the two buttons **Pull from system** and **Display** is the same as the output of the `conf -long` command.

### 2.14.2.7 HealthPage "Software Subsystem" example

The Software Subsystem is divided into two categories. Software subsystems used by the AWS Platform and Application, and those essentially used for Service Tools.

In the example below, an external License server is used (the site is not using the internal license server).

Software Subsystem	Status
EC-Workspace (workspace-bundle)	OK
EC-Navigator (navigator-bundle)	OK
EC-Worklist (worklist-bundle)	OK
EC-Preview Pane (preview-pane-bundle)	OK
EC-Dicom Web Service (dicomweb-service)	OK
EC-XE Service (xe-services)	OK
IF-Imaging Fabric (imaging-fabric)	OK
IF-Setup Operator (setup-operator)	OK
EML-Central Configuration Store (eml-CCS)	OK
EML-Certificate Management Service (certificate-management-service)	OK
EML-Filewatcher Service (file-watcher-service)	OK
EML-Centralized Logging Service (eml-fluentbit)	OK
EML-Security Auditing Service (ees-security-auditing)	OK
EML-Postgres Service (ees-common-postgres-service)	OK
EML-Messaging Service (ees-rabbitmq-service)	OK
EML-Docker (Docker)	OK
EML-Helm (Helm)	OK
EML-Kubernetes (Kubernetes)	OK
ComponentRegistration en_US (component-registration)	OK
Image Management Subsystem (nuevo)	OK
Firewall (pnf)	OK
Audit Server (eat)	OK
Authentication/Authorization Server (ea3)	OK
Application Interoperability platform (dotmedservice)	OK
Super Server (aweservice)	OK
Client exporting subsystem (rmp-server)	OK
Built-in License Server (cola-server)	Unused
Printing Service (prserver)	OK
Preprocessing (xpreproc)	Unused
Integration Service (pacsinteg-webservice)	Unused
Time Server (chronynd)	Unused
DICOM Direct Connect (tomcat@ddc)	Unused
Media Creator (mediacreator-app)	OK
Configuration Service (configuration-service)	OK
MailSender Service (mailsender-service)	OK
Application Service (application-svc)	OK
Applist Service (applist-svc)	OK
End of Review Service (endofreview-svc)	OK
Visualization Service (visualization-svc)	OK
Authentication Service (auth-service)	OK
IDP (Keycloak) Service (keycloak)	OK
Software Download (irisd)	OK
ELS Service (els)	OK
Certificate Management Service (cm-service)	OK
<b>Restart</b>	
Restarting these services should only be performed by a qualified service or IT operator. (Maintenance mode is required)	

Software Subsystem essential for Service Tools	Status
httpd	OK
tomcat	OK
rmiregistry	OK
servicermi	OK
awservicermi	OK
<b>Refresh All</b>	

#### NOTE

The **Restart** button is provided to restart the services, in case some of them would report an error condition. You may use this feature to avoid rebooting the server.

Using the **Restart** button should be used cautiously when the AW Server is in use, as it may disconnect the Users.

### 2.14.3 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, as shown below.

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.



#### NOTE

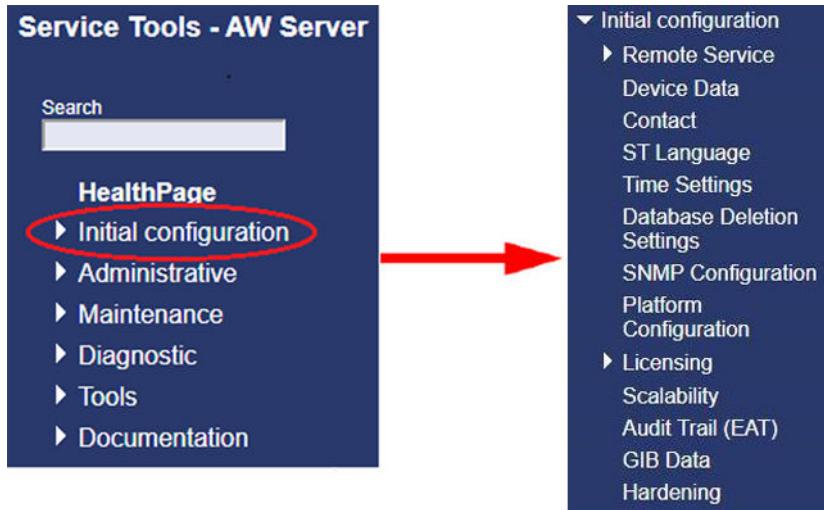
**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

Proceed to [2.15 Job Card IST008 - Initial Configuration on page 140](#).

## 2.15 Job Card IST008 - Initial Configuration

- From the Service Tools menu, click on **Initial configuration** to expand the menu.



### 2.15.1 Configuration - Cluster case

#### NOTE

If using the Installation Wizard (Cloud-init mechanism), skip this section as the configuration is performed using the configuration file generated by the Installation Wizard.

- In case of cluster mode, speed up the current node (AW Server) configuration by:
  - Backing up the configuration of the first node fully configured and licensed.  
Refer to section [3.10.3.3 Backup the Site configuration on page 503](#).
  - Restoring the backup previously created on the current node.  
Refer to section [3.10.6.2 Restoration steps on page 527](#).

#### NOTE

During the restoration, a message will popup mentioning that the license ID of the system does not match with license ID in the back up file, as the backup has been done from another AW Server.

#### NOTE

Most of the Initial configuration (this Job Card) and Administrative configuration ([2.18 Job Card IST010 - Administrative Configuration on page 184](#)) will be restored.

- When the restoration is complete, set the correct **System ID** (System ID of the current node) in **Initial Configuration > Device Data**.
- Proceed to the [2.15.9 Platform Configuration on page 153](#).
- Proceed to the [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#).
- Proceed to the [2.15.10 Licensing Configuration on page 156](#).
- Continue the node (AW Server) installation/configuration as for the first node.

#### NOTE

Platform configuration is not restored as well as the platform license and applications licenses as the backup has been done from another AW Server.

## 2.15.2 Remote Service

### 2.15.2.1 RSvP Remote Service (GEHCS only)

#### NOTE

If the Secured for RMF mode is planned to be activated, do not perform this procedure.  
Remote connectivity is not supported in RMF mode.

In the top banner, if RSvP is not properly configured or not running, a message is displayed with the “[Click here for details](#)” link, which brings you to the RSvP configuration panel described below.



#### NOTE

For information, the RSvP model type for AW Server 3.2 is: **AWS32\_RSVP**.

#### 2.15.2.1.1 RSvP Remote Service setup

- From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration**.

The **Configure RSvP Agent** panel displays.

Configure RSvP Agent	
<a href="#">Overview</a>	
<b>Agent</b>	<b>Status</b>
Running	No
Connected	Unknown
Registered	Unknown
CRM Verified	Unknown
Quarantine	Unknown
Connection time	Unknown
<a href="#">Refresh</a> <a href="#">Start</a> <a href="#">Stop</a> <a href="#">Restart</a>	
<b>Agent</b>	
System ID (CRM Number) *	<Mandatory>
Serial Number *	<Mandatory>
Display Name	
Model Number *	AWS32_RSVP
Version	2.3
<b>Enterprise Server</b>	
Hostname / IP *	insite.gehealthcare.com
Port Number *	443
<b>Proxy Server</b>	
Hostname / IP	
Port Number	
<small>* Mandatory fields</small>	
<b>Feature</b>	
Prodiags	Enabled

2. Select the **Settings** tab.

Configure RSvP Agent	
<a href="#">Overview</a> <b>Settings</b> <a href="#">Features</a>	
<b>Agent</b>	<b>Configuration</b>
System ID (CRM Number) *	AWBUCLAB243
Display Name	
<b>Enterprise Server</b>	<b>Configuration</b>
Name	Production
Hostname / IP *	insite.gehealthcare.com
Port Number *	443
<b>Proxy Server</b>	<b>Configuration</b>
Hostname / IP	PITC-Zscaler-EMEA-Amster
Port Number	80
Username	*****
Password	*****
* Mandatory fields	
<a href="#">Refresh</a> <b>Save</b> <span style="border: 1px solid red; padding: 2px;"> </span> <a href="#">Restart</a>	

3. In the **Agent** table, enter the **System ID (also defined as CRM NUMBER)**.

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

4. In the **Enterprise Server** table, enter the **Name** of the RSvP server.

**NOTE**

There are two Enterprise Server, one in the US (e.g.: **Production**) and one in EU (e.g.: **Production-EU**). Use the one which is close to your location.

5. In the **Proxy Server** table, if the customer use a Proxy:

- Enter the **Hostname / IP** of the Proxy server.
- Enter the **Port Number** of the Proxy server.
- Enter the **Username** and **Password** of the Proxy server.

**NOTE**

This information can be acquired from the customer IT admin.

6. Click on **Save** button to save the RSvP settings.

**NOTE**

Use the **Refresh** button to reset the settings to the previous values entered.

Use the **Restart** button to restart the RSvP Agent.

7. In the **Overview** tab, review the RSvP settings.

Agent	Configuration
System ID (CRM Number) *	AWBUCLAB243
Serial Number *	AWBUCLAB243_20210201_183831
Display Name	AWBUCLAB243-Test
Model Number *	AWS32_RSVP
Version	2.3
Enterprise Server	Configuration
Hostname / IP *	insite-eu.gehealthcare.com
Port Number *	443
Proxy Server	Configuration
Hostname / IP	PITC-Zscaler-EMEA-Amsterdam3PR.proxy.corporate.ge.com
Port Number	80

\* Mandatory fields

8. Click on **Start** button to start the RSvP Agent.

The **Running** status turns green.

Agent	Status
Running	Yes
Connected	No
Registered	No
CRM Verified	No
Quarantine	No
Connection time	N/A

#### NOTE

Use the **Stop** button to stop the RSvP Agent.

Use the **Restart** button to restart the RSvP Agent.

9. Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green (except for the **CRM Verified** status - see [2.15.2.1.2 System ID \(CRM Number\) verification on page 144](#)).

#### NOTE

Do not hesitate to select the **Refresh** button again till the status turns green (see below status definition and latency to turn green).

Agent	Status
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	No
Quarantine	No
Connection time	Mon 1 Feb 2021 06:43:30 PM GMT+1

Status definition:

- **Running:** Value is **Yes** if the Agent is running. Otherwise, the value is **No**.
- **Connected:** Value is **Yes** if the Agent can be registered to the back office and is actively polling the back office. If the Agent is unable to successfully poll the back office, the value is **No**.
- **Registered:** Value is **Yes** if the Agent has successfully registered with the back office and has received confirmation of this registration. Otherwise, the value is **No**.

This value does not reflect if the Agent is actively polling. It is a 1 time notification of successful registration.

To see if the Agent is currently communicating with back office, see the **Connected** status.

#### **NOTE**

The **Yes** status may take a minute or two to appear.

- **CRM Verified:** If the value is **Yes**, it means that the System ID (a.k.a. CRM Number) is in CRM systems. Otherwise, the value is **No** (see [2.15.2.1.2 System ID \(CRM Number\) verification on page 144](#)).

#### **NOTE**

The **Yes** status may take up to 5 minutes to appear.

- **Quarantine:** Value is **Yes** if the Agent is currently in Quarantine. Otherwise, the value is **No**. If Agent status returns quarantine values as **Yes**, it means that RSvP back office cannot uniquely identify the device as some other device is also running an agent using the same System ID (CRM Number).

#### **NOTE**

The FE shall contact the RSvP team to resolve the issue.

- **Connection time:** Value is the last successful connection date/time of the RSvP Agent with the back office.

#### **NOTE**

The RSvP status is also displayed in the **Remote Service** table of the Healthpage.

## **2.15.2.1.2 System ID (CRM Number) verification**

#### **NOTICE**

It is important to have the System ID (CRM Number) verified now, so that the system will be able to upload its configuration to the AWCCT website and automatically receive in return the Registration Configuration key, necessary to enable the AW Server.

#### **NOTE**

Registration will have to be done manually if RSvP is not available.

#### **NOTE**

Without the Registration key, the AW Server will not allow exiting from the Maintenance mode and therefore be accessible to the Clients.

1. From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration**, check that the status of the RSvP Agent are green.

Agent	Status
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	Yes
Quarantine	No
Connection time	Mon 1 Feb 2021 07:46:44 PM GMT+1

2. If the **CRM Verified** status remains red, select the **Refresh** button to refresh the RSvP Agent status.

As mentioned in previous section, the **CRM Verified** status takes time to turn green.

If it remains red after 5 minutes, contact the local RSvP team to get the System ID (CRM Number) verified for the system.

When all the RSvP Agent status are green, the system is ready to be accessed remotely.

3. Proceed to the connection tests with FFA, to make sure the system is ready to be accessed remotely.

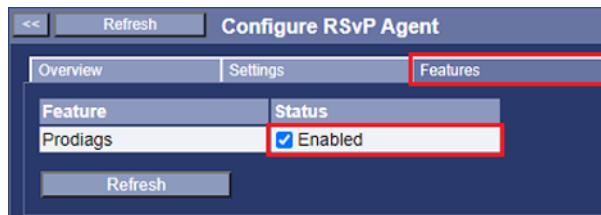
### 2.15.2.1.3 Prodiag configuration

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

#### NOTE

Bypass this step if the site is a GE PACS (CPACS, IW/Universal Viewer, EA) site. GE PACS does not use RSvP and Prodiag needs an operational RSvP connection to work.

1. In Service Tools, select **Remote Service > RSvP (GE Backoffice) Configuration** and select the **Features** tab.



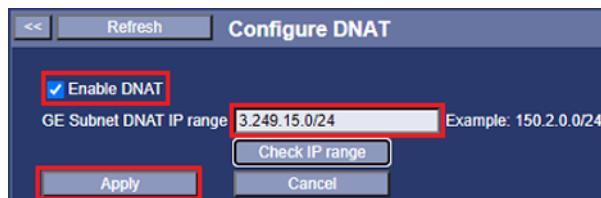
2. The Prodiag feature is enabled by default.

To disable the Prodiag feature, uncheck the **Enabled** check box. The message Success (on a green background) displays briefly.

### 2.15.2.1.4 Configuring DNAT

Sites using DNAT do not see the GE back office on the IPs that are statically set up in the PNF (150.2.0.0/16, 10.190.64.0/24, 82.136.152.0/24). Service user can configure the DNAT IP range that is used to access GE in the DNAT page.

1. From the Service Tools, select **Initial configuration > Remote Service > DNAT**.



2. Select the **Enable DNAT** check box to enable.
3. Enter the **GE Subnet DNAT IP range** (format example displayed on the tool).
4. Click on **Check IP range** button to check the IP range. The message Success (on a green background) displays briefly.
5. Click on **Apply** button to save the configuration.

### 2.15.2.2 EDS Remote Service

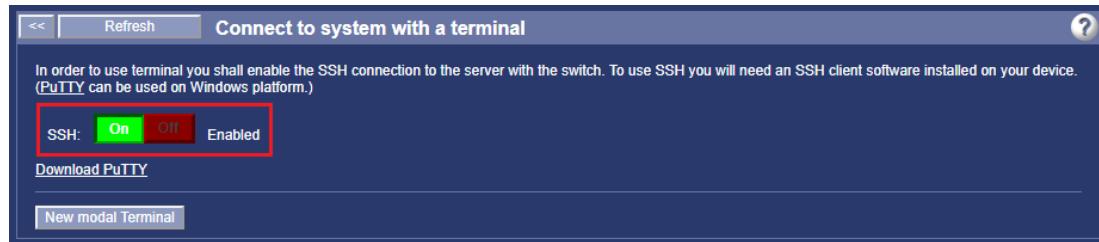
#### NOTE

Not applicable in Secured for RMF mode.

This must be done for EDS systems only.

1. Open the SSH port to allow remote access.

- a. Select **Tools > Terminal** button.
- b. Click on the SSH **ON** button.
- c. Check the message **Enabled** displays.



2. Alternate step: Click on **New modal Terminal** and on **Connect**. Login as **root** and type in the terminal:

```
ssh_enabler -enable <Enter>
```

#### NOTICE

It is recommended that GE HCS sites using remote service keep the SSH button set to **OFF** in order to disable SSH for increased security.

### 2.15.3 Device Data

All site information must be available for remote use and for other system tools to query.

1. Get the device information from the site IT Admin.
2. In Service Tools, select **Initial Configuration > Device Data**.

The *Set device and hospital specific data* panel appears.

3. Enter the site information:

All mandatory fields (marked with an asterisk (\*)) must be filled out to obtain the Configuration Registration key.

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

**NOTE**

If the **System ID (CRM Number)** is not set, select **Configure System ID** link to set this field through the RSvP Agent configuration pages. Refer to [2.15.2.1.1 RSvP Remote Service setup on page 141 Step 1 to Step 3](#) and click on the **Save** button.

4. Enter one of the following in the **Service area** field:
  - APAC for Asia / Pacific
  - EU for Europe
  - LA for Latin America
  - CH for China
  - IN for India
  - USCAN for US / Canada
  - EAGM for Eastern & Africa
5. Click on **Apply**.

## 2.15.4 Contact Data

You must enter customer contact data for the site.

1. From the **Service Tools**, select **Initial Configuration > Contact**.

The *Set up contact info* interface displays with three default contact names: **Hospital IT**, **GE Contact** and **Hospital admin**.

2. Select each contact from the above list and enter as much of this contact information as possible in their form. Enter at least their **Name** and **Phone** number. The contact information is critical for remote service.

3. Click on **Apply** to save the information.
4. To add additional contacts, click on the **Add** button, then fill in the necessary information. This information will also be retained with the Administrative Backup / Restore tools.
5. Click on **Apply** to save the additional contacts.

## 2.15.5 Service Tools Language (for Administrator)

You must enter the Interface language for the "Administrator" and the "Standard" users of the site.

Note that for the GEHC Service user, the Interface remains in English only.

1. From the *Service Tools*, select **Initial Configuration > ST Language**.
2. Use the drop-down menu to select the **Service Tools language** for the site.

Default is **English**. The site order should specify which Service Tools language is to be set.



3. Click on **Apply** to save configuration.

## 2.15.6 Time Settings

You must verify that the time was set correctly during the installation of the system, and make corrections if needed.

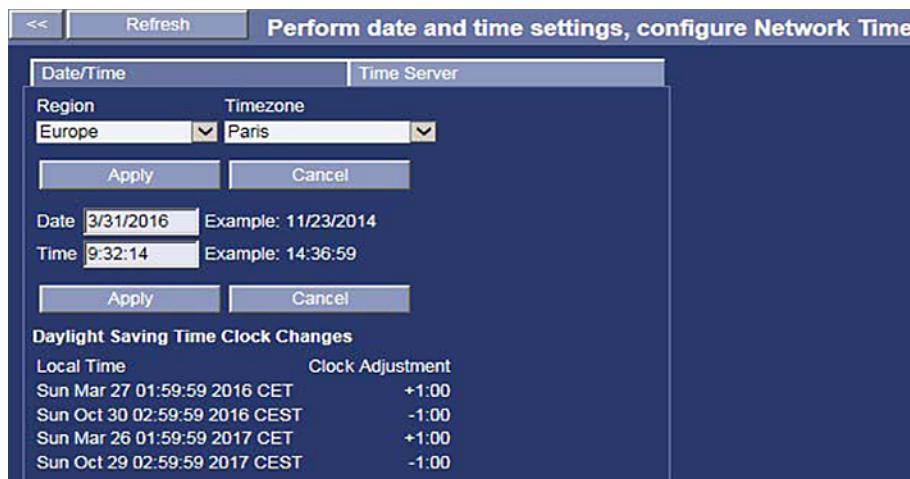
### NOTICE

Consult with the site's IT administrator before changing any data for time settings!

### 2.15.6.1 Date and Time menu

1. From the *Service Tools*, select **Initial Configuration > Time Settings**.

The *Date/Time* and *Time Server* tabs display.



2. In the *Date/Time* tab, verify that each field has been set correctly. If any field is incorrect, change it to the correct value.
3. Click on **Apply** to save the information.

## 2.15.6.2 Time Server menu

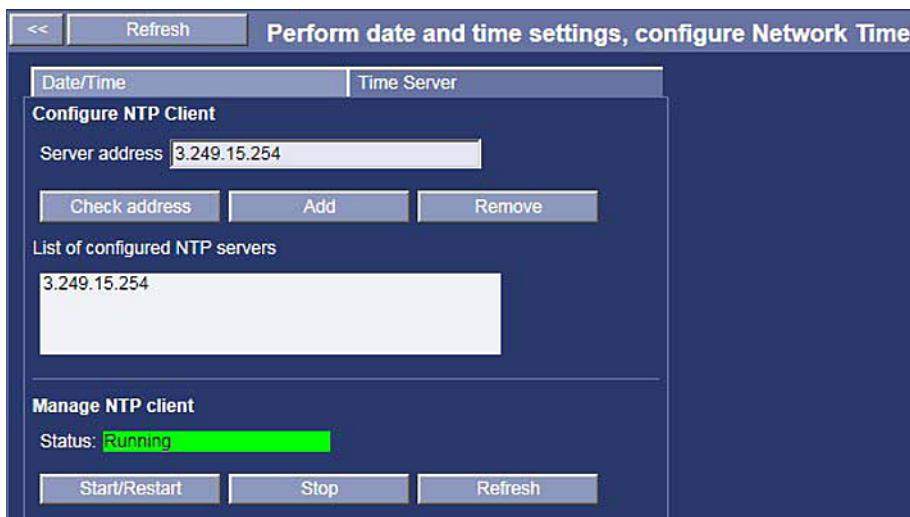
### NOTICE

NTP is not aimed to correct an invalid time but to keep a basically correct date/time in sync with the NTP server. First make sure Date and Time have been correctly setup for your site. You must have performed steps described in previous section.

### NOTICE

Using a Time Server is a "MUST" for Scalability. If your virtual AW server is going to be part of a cluster of AW servers, you need to setup a NTP server.

1. If your site is going to use a Time Server, select the *Time Server* tab.



2. To add a NTP server to the *List of configured NTP servers*, enter the NTP server's IP address in **Server IP address**.

### NOTE

For virtual AW Server, use the same NTP server IP address than the one which was set in the hypervisor. Refer to [2.8.3.4 NTP server setup for the Virtual AW Servers / HAPS servers on page 84](#).

3. Check the NTP server's IP address:

- a. Click on **Check address**.
- b. Click on **Add**.

After a few seconds, the Status window should report Running.

### NOTE

If DNS servers have been previously configured, it is possible to enter the Hostname(s) instead of the IP address(es) of the NTP Server(s).

### NOTE

Use the **Remove** button to remove a NTP server, then click on the **Refresh** button on the HealthPage to refresh the Service Tools information.

**NOTE**

NTP server MUST be setup for all servers. This is a mandatory step. You are not able to exit the Maintenance mode as long as NTP time synchronization is not configured.

## 2.15.7 Database Deletion Settings

### 2.15.7.1 Auto Delete settings

Check with the customer or the IT administrator if they would like the Auto Delete feature to be turned on.

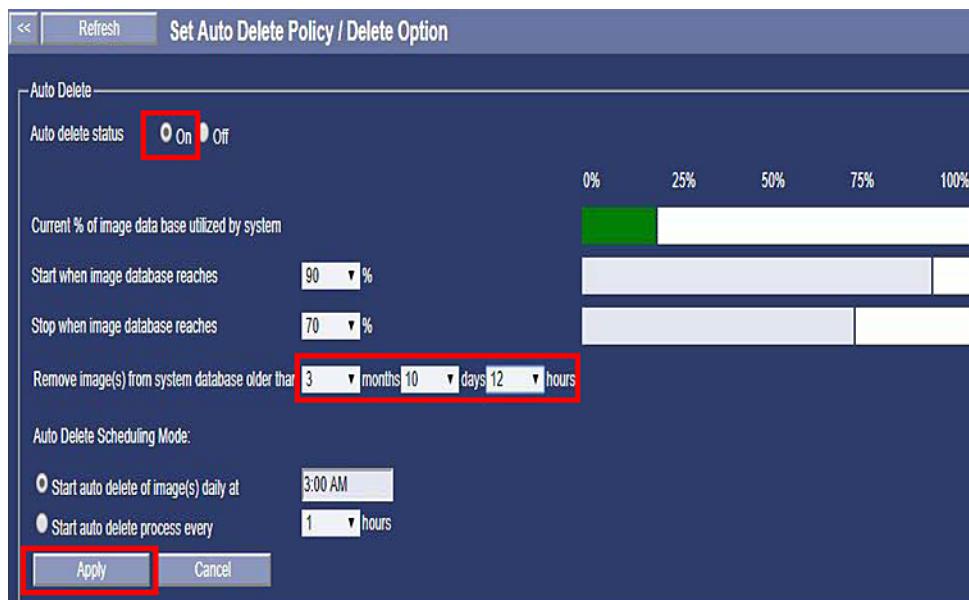
The Auto Delete feature is disabled by default but you must enable it for Full, Seamless or DICOM Direct Connect Integration (GE-PACS case).

**NOTE**

Exam can be auto-deleted when (criteria and order):

1. Storage commitment flag is set for that exam at study level (whole exam archived),
  2. Or exam has derived images but storage commitment flag has been set,
  3. Or exam does not have any derived images
  4. Or exam has derived images but are older than the specified age.
1. From the Service Tools, select **Initial Configuration > Database Deletion Settings**.

The *Set Auto delete Policy / Delete Option* interface displays.

**NOTE**

Do not be alarmed to see that the bar graph shows that there is already some space utilized in the **Current % of image database utilized by system**, even though there are not yet patient data stored. The space available for images is less than the space allocated for images. This is due to the AW Server software reserving some space for internal management (e.g: database storage, temporary files...).

2. Check the **On** radio button.
  3. Select the age (in months and/or days and/or hours) of data candidate for deletion
- For example: 0 month ; 15 days : 12 hours.

4. Chose the **Auto Delete Scheduling Mode**: either set the start time of the auto-delete process, or set the frequency of the auto-delete process.
5. Keep the other settings to the factory default values unless otherwise specified. For sites using the AW Server intensively, preferably set the High watermark lower than 90% (80% is recommended), to avoid exceeding the high watermark limit and filling up the disks before auto-delete is started.
6. Click on **Apply** to save the configuration.

**NOTE**

For Seamless and DICOM Direct Connect integration, all exams are on the PACS. Only processed images are stored on the AW Server then automatically sent to the PACS.

### 2.15.7.2 Delete option for worklist browser

Check with the customer or the IT administrator if they would like the Delete option for worklist browser feature to be turned on.

This feature is set to disabled by default. When this option is enabled, all users (except **limited** user) are able to delete selected studies or series from the worklist browser.

**NOTE**

This does not apply to integrated systems, where the database is at the PACS side.

1. From the **Service Tools**, select **Initial Configuration > Database Deletion Settings**.

The *Delete option for worklist browser* interface will display at the lower side of the menu.



2. To enable the Delete option, check the **On** radio button.
3. Click on **Apply** to save the configuration.

### 2.15.8 Configuring SNMP

**NOTE**

If the Secured for RMF mode is planned to be activated, then do not perform this procedure, keep SNMP in **Disabled** state. SNMP feature is not supported in RMF mode

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

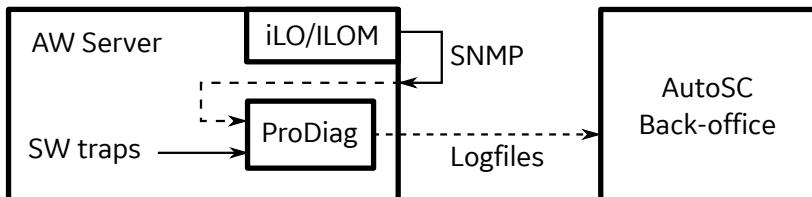
This application works in the background and has neglectable effect on available resources.

SNMP monitors data (SNMP traps) locally, on the AW Server, and sends messages to the SNMP server (SNMP trap receiver) in case of failure.

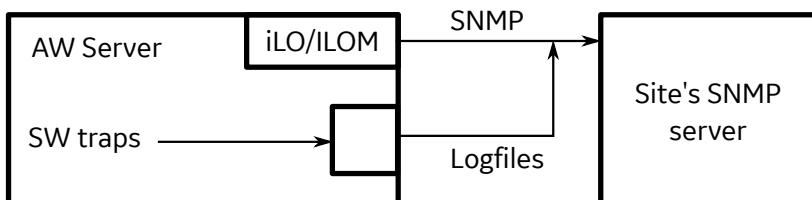
- By default, the AW Server acts as an SNMP server.
- If ProDiag is used, the data are sent to the GE back-office using ProDiag messages.

- If the site's SNMP server is configured, the data are sent to it as well.

SNMP configuration with ProDiag



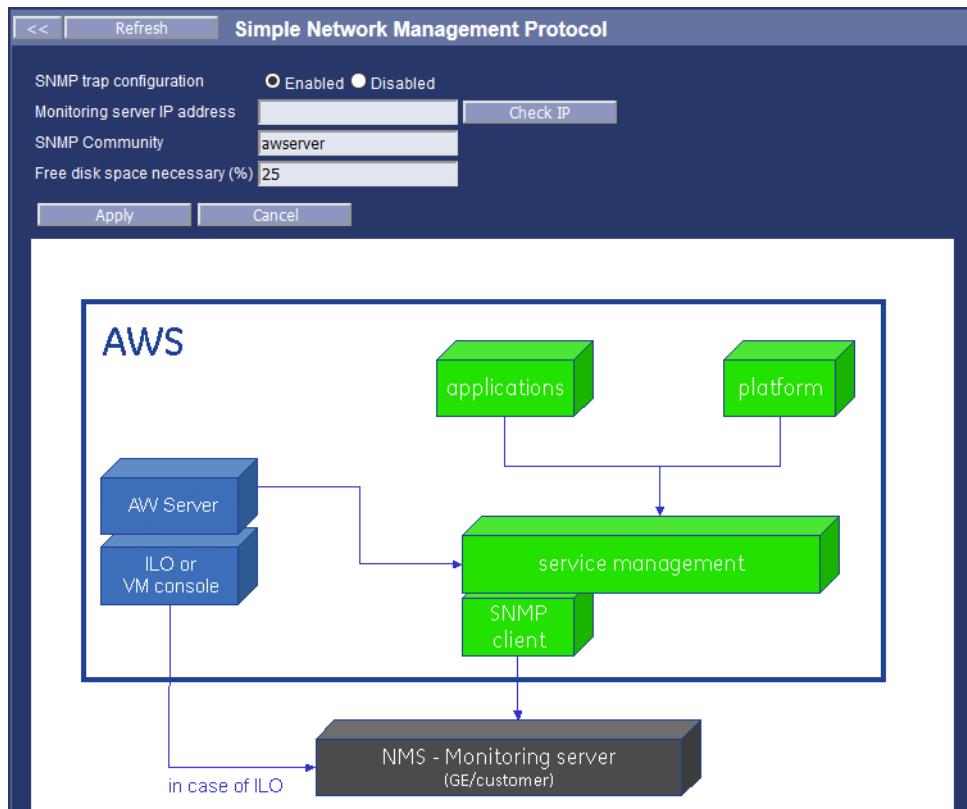
SNMP configuration with site's SNMP server

**NOTE**

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

To configure SNMP:

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

**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.

## 2.15.9 Platform Configuration

### 2.15.9.1 Licensing Preparation

The system licenses are not created by GEHC manufacturing and need to be created by the GEHC FE or by the OLC for the FE.

The licenses are created at installation time based on the license ID of the AW Server, which is calculated by the Platform Floating License Client Configuration tool, and displayed under **Platform Configuration**.

1. Write down the license ID & the site GON (Global Order Number).

The license ID is available from the **HealthPage** or from **Initial Configuration > Platform Configuration**.

The GON is listed on the site's paperwork from GEHC.

2. Access the GEHC eLicense website (see [A.3 Licensing on page 556](#) for details).

<http://elicense.gehealthcare.com/elicense/> OR <http://elicense.gehealthcare.com/> - this URL is available via the Internet, and via the GEHC VPN connectivity model.

#### NOTE

If you can't connect to eLicense, contact the OLC and ask them to obtain the licensing information for you.

3. Query the GON, and create the license keys for the catalog entries in the GON that show up as license key enablers –

- **AWS Primary** is the correct model type for AW Server 3.2 hardware or virtual server.
- **AWS Node** for the other virtual AW Servers in the cluster.

**Platform Enabler** – this is the number of slices related to the specific catalog node-locked server license.

**Server Enabler** – node-locked AW Floating License Manager license (CoLA License Server - if applicable). The Server Enabler key licenses the AW Server to run a “built-in” Floating License Server for itself. This does not exist or is not needed if the server is configured to use “external” floating license server(s) at other IP address(es).

4. Copy or download the licenses and/or config.txt file from eLicense.

For the initial platform software installation, you must manually enter the license numbers into the Platform Enabler and Server Enabler fields.

## 2.15.9.2 Configuration Steps Summary

The platform configuration is composed of three steps corresponding to three tabs. To be able to save the configuration, you must complete each tab in the following order:

- The *Platform Configuration* tab to select the number of slices supported by the hardware platform and enter the corresponding license key.
- The *Scalability* tab to setup whether or not the system is to be placed within a cluster of other AW Server (only applicable to virtual AW Server). It is not intended to configure Scalability. This is done later through the Scalability menu and is covered by Job Card [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#).
- The *Integration* tab to setup the Integration mode.

The PACS/RIS Integration configuration is covered by Job Card [2.19 Job Card IST011 - Integration on page 221](#).

The platform configuration settings are saved only after going through the *Scalability* tab and *Integration* tab by clicking on the **Next** button of each tab.

Pre-requisite for Seamless integration

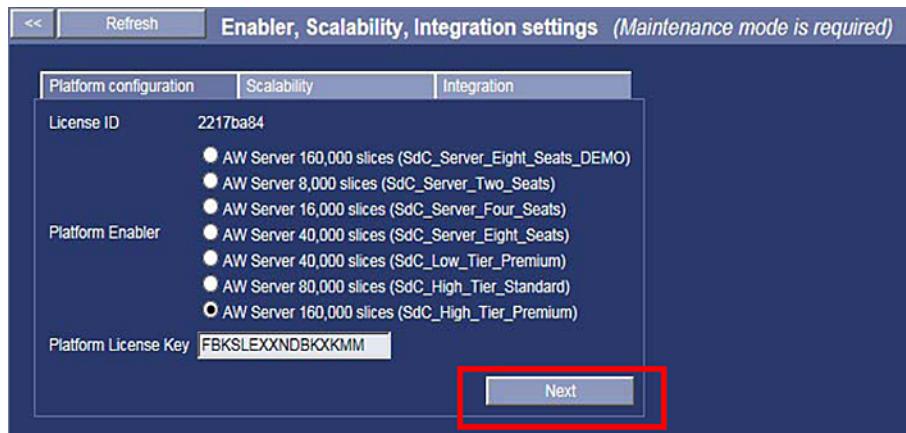
### NOTICE

If your site is going to be integrated to the Universal Viewer (Seamless integration), proceed with the Dakota plugin loading prior to proceed with the Platform Configuration steps. Refer to section [2.19.3.4 Seamless integration - configuration steps on AWS, Service Tools on page 231](#). When done, proceed with next section:

## 2.15.9.3 Platform configuration menu

1. From the *Service Tools*, select **Initial Configuration > Platform Configuration**.

The *Enabler, Scalability, Integration settings* page displays similar to the example below:

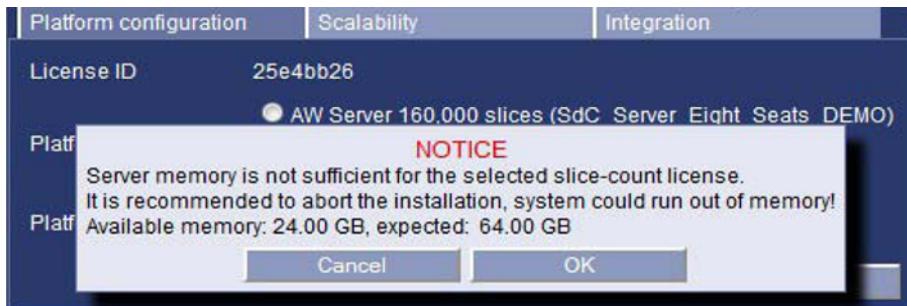


2. If the server is not in Maintenance mode, the following message displays:



Click on **OK** to acknowledge and place the server in Maintenance mode before resuming.

3. Click on **OK** to allow the installation or **Cancel** to abort and fix the issue first.



#### **NOTICE**

In case the server would not be fitted with the appropriate size of memory, or in case some part of the memory would be defective, installation can be allowed, but the issue should be fixed as soon as possible, and the customer warned that performances could be degraded. A message such as the following example will display:

4. Choose the correct **Platform Enabler** description.

Refer to [2.3.1 Physical AW Server Characteristics on page 32](#) and [2.4.1 Virtual AW Server Characteristics on page 36](#).

The system's GON (Global Order Number) should identify the license related to the number of slices.

#### **NOTE**

The AW Server 160,000 slices DEMO entry is dedicated for demo units. These demo units do not require to be registered. However, they permanently display a banner mentioning that the system shall not be used for diagnostic.

#### **NOTE**

The reference to Seats is rather a functional limitation related to the number of slices available to be processed by all users, than a number of users limitation.

5. Record the License ID number for future use.
6. Enter the **Platform License Key** for your AW server.

Click on the **Next** button to display the **Scalability** tab.

### **2.15.9.4 Scalability setup menu**

1. In the **Scalability** tab, select whether or not your AW Server (virtual AW Server only) is placed into a cluster of virtual AW Servers by clicking on the **Cluster Mode** or **Single Mode** radio buttons.



### NOTICE

The Cluster mode is not available for physical hardware AW Server.

- Enter the IP address for each HAPS server.

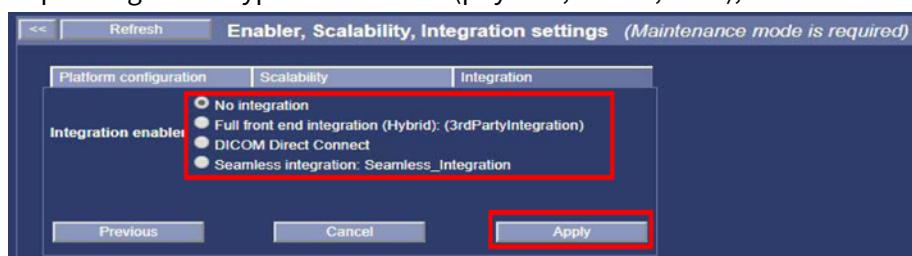
For more detailed information, refer to [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#).

Click on the **Next** button to display the *Integration* tab.

## 2.15.9.5 Integration configuration menu

- In the *Integration* tab, select whether or not your AW Server is integrated to a RIS or PACS and what type of integration is used by clicking on one of the following radio buttons:
  - No integration** (standalone)
  - Full front end integration (Hybrid): (3rdPartyIntegration)**
  - DICOM Direct Connect**
  - Seamless integration: Seamless\_Integration**

Depending on the type of AW Server (physical, virtual, etc ..), all choices may not display.



### NOTE

Configuration of Integration is an important step consisting on several configuration steps, both on the AW Server and on the PACS. As an alternative, if you are not yet sure of all the Integration configuration parameters, we recommend that you temporarily keep the **No integration** button selected, and setup integration later on, as detailed in [2.19 Job Card IST011 - Integration on page 221](#). However, if the software detects that you are installing a 16K slices key on a virtual AW Server, you will be prompted to setup the Seamless integration at this time (the 16K slices key on vAW Server is only commercialized for Seamless Integration).

- Click on the **Apply** button to save the settings.

### NOTE

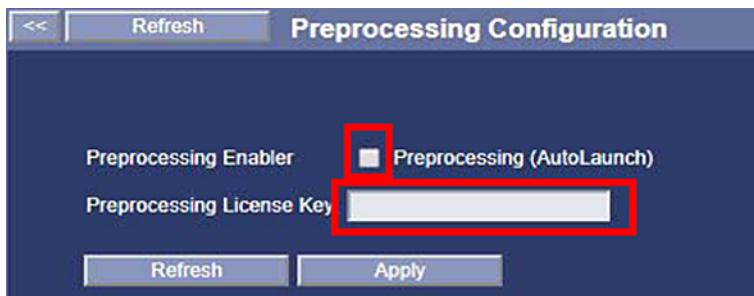
You do not need to reboot the server at this time, as prompted in the message. Reboot is only necessary when you have completed all Integration setup steps.

## 2.15.10 Licensing Configuration

## 2.15.10.1 Preprocessing configuration menu

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

The **Preprocessing Configuration** panel displays:



2. Click on the **Preprocessing (AutoLaunch)** checkbox to enable the feature.
3. Enter the **Preprocessing License Key** for your AW server.

**NOTE**

This license key is required for the client to access the Autolaunch advanced application..

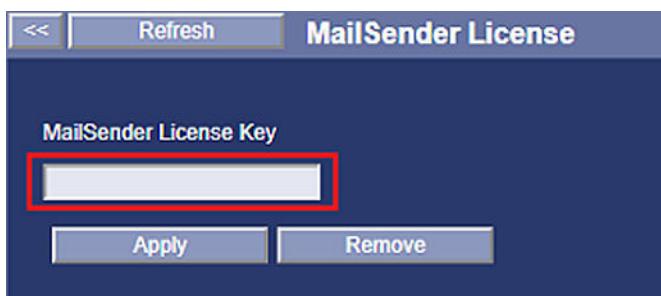
4. Click on the **Apply** button to save the configuration.

## 2.15.10.2 MailSender

This license key is required to allow applications to send email reports to predefined recipients.

1. In Service Tools, select **Initial configuration > Licensing > MailSender**.

The **MailSender License** page displays:



2. Enter the **MailSender License Key**.
3. Click on the **Apply** button to save.

## 2.15.10.3 CoLA License server

AW Server is shipped with one Floating License (FL) server license key.

AW server has an internal License server feature, so it can be used as License server for Applications.

It is recommended whenever possible to use external license server(s), as any potential downtime of the AW Server would mean downtime of the internal FL server. Any Client PCs and other system requiring to be served with floating licenses would be impacted in that case.

If the Secured for RMF mode is planned to be activated, then use the internal CoLA server. External License Server is **not allowed** in RMF mode.

External license servers are recommended when the site has several devices using Floating License. If it is an AW Server alone, then it is recommended to use the internal CoLA server.

**NOTICE**

No CoLA software package is provided to load any external FL server. If the customer wants to install an external Floating license server, he/she has to order the software package CAT # M81171SW, and purchase CAT # M80171LS pulling the AW Floating License Manager license key. In case of upgrade, the following shall be purchased: CAT# M81171SV AW Floating License SW Upgrade.

**High Availability option:**

This option provides a secondary license server for the AW Server in order to create a highly available licensing solution. Connect to the eLicense web site <http://elicense.gehealthcare.com>, select the User Guide section and open the AW-eLicense Service Manual.

You will have to look at the instructions related to the High Availability Option in the AW-eLicense Service Manual.

Also refer to **5724192-1EN** - AW Server High Availability Read Me First, for details.

### **2.15.10.3.1 CoLA License server installation**

If the Floating License Server(s) is (are) not already installed on your site, you must install it (them) now.

New License servers can be installed either on Physical hardware platforms or on Virtual Machine platform.

The OS supported are Windows 7, Windows Server 2008 and Windows Server 2012.

Refer to **5537368-1EN - Floating License 3.3.x Installation Manual** for details.

1. Insert the documentation CD into the DVD drive of the customer's PC that is used as License Server PC.
2. Drag and drop the Floating License 3.3.x Installation Manual PDF file on the PC desktop.
3. **NOTE**

The following information may change depending on any eventual update of the Floating License 3.3.x Installation Manual.

Read Section 1 - Introduction and Section 2 - Installation overview Sections 2.1 and 2.2 of the Floating License 3.3.x Installation Manual.

4. Eject the documentation CD and insert the Software CD instead.
5. Proceed with the Floating license software installation following Section 3 up to Section 3.4.

**NOTE**

Bypass Sections 3.5 to 3.8 of the Floating License Installation Manual. They are only applicable to the Advantage Workstation, not to the AW Server.

6. Follow steps described in Section 3.9 to access the eLicense site and enter the licenses in the Floating License server(s).

### **2.15.10.3.2 CoLA License server configuration menu**

- To use the built-in server, you need the license key.
- To use External License Server(s), you need the IP address(es) and port number from the IT admin.

**NOTE**

The status of the built-in Floating License server is also indicated on the *Service Tools HealthPage* in Built-in License Server (cola).

Software Subsystem	Status
Image Management Subsystem (nuevo)	OK
Firewall (pnf)	OK
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

- The green OK message means the Server Enabler is valid and is running.
- A red message means it is failing in some way.
- The grey Unused message means it is not selected and not being used.

1. In Service Tools, select **Initial configuration > Licensing > CoLA Server**.

The *CoLA Server Configuration* panel displays.

2. For Internal License Server case, follow [Step 3](#) to [Step 7](#). For External License Server case, follow [Step 8](#) to [Step 14](#).

**Internal License Server case:**

3. If you have received a license key for the built-in server and do not have a cluster of virtual AW Servers, check on the **Built-in** checkbox.



4. Enter the Server Enabler license key in **Server Enabler**.

5. Keep the other default settings:

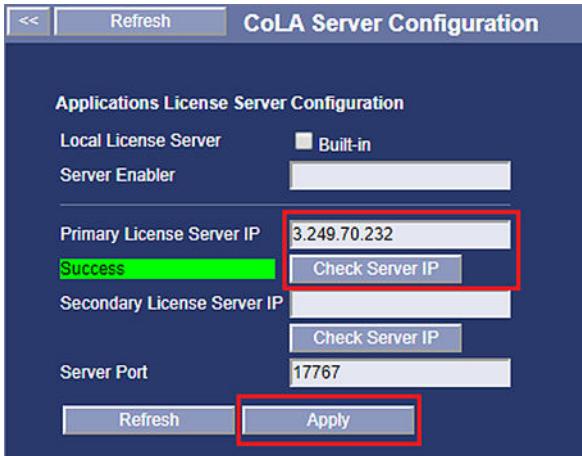
**Primary License Server IP: 127.0.0.1**

**Server Port: 17767**

6. If applicable for your site, configure the Secondary License Server.
7. Click on the **Apply** button to save the configuration.

**External License Server(s) case:**

8. Uncheck the **Built-in** checkbox.



9. Enter the **Primary License Server IP** address.
10. Enter the **Server Port** number if it is different from the default **17767** value.
11. Check the Primary Server by clicking on **Check Server IP**.
12. If applicable, enter the **Secondary License Server IP** address.

**NOTE**

The Secondary License Server can be either the AW Server internal License Server (built-in) or an external License Server. The Second License Server shall only be configured if your site has purchased the CoLA High Availability option.

**NOTICE**

It is NOT ALLOWED to combine Primary license server and Secondary license server, that is to say, all AW Servers of the site (or in the Cluster) must use the same license server as Primary server, and the other server as Secondary. It is under the GEHC FE full responsibility not to mix the License servers.

13. Check the Secondary Server by clicking on **Check Server IP**.

Scalability case:

Preferably install External (CoLA) License Servers on physical machines different from those hosting a VM (virtual machine). If it is not possible, one of the AW Server's VM built-in (CoLA) server can be used as Primary License Server, and another AW Server's VM built-in (CoLA) server can be used as Secondary License Server, but this is not recommended.

There are two model types in eLicense: AW\_primary and AW\_Node.

You receive the license keys for the External CoLA License Server only with one AW Server considered as AW\_Primary. All the other servers in the same cluster are considered as AW\_Node and do not receive license keys for External CoLA License Server.

14. Click on the **Apply** button to save the configuration.

## 2.15.10.4 Floating License – Application licensing

This section describes how to license the Advanced Applications. These licenses are based on the License ID and are generated using eLicensing tool. Refer to [A.3.1 eLicense licensing on page 556](#).

The AW Server can be its own (built-in) Floating License Server or it can use an (external) Floating License server when installed at the customer site.

The Floating License Manager tool does the following:

- Displays the “Target Server” information:
  - License ID - Name/IP Address - Hostname - Version
  - Server Enabler license key string and license key
- Displays licenses on the FL Server, and number of users

When using the built-in FL server, the listed licenses are on the AW Server. They can be entered manually or read from a portable media or file location (eLicense config.txt file) to UPDATE the server.

When using an external server, the listed licenses are read from the external server.

1. Make sure the internal Floating License server has been properly setup with its license, or that the External license server(s) is operational and populated with the appropriate licenses. Refer to section [2.15.10.3 CoLA License server on page 157](#).

If the Cola license has not been installed yet, you will not be able to setup the Applications licenses, that will report an error upon installation.

2. From the Service Tools menu, click on **Initial configuration > Licensing > Floating License**.

The GEMS Floating License Manager menu displays as in the example below:



### NOTE

If many application licenses are to be installed, you may have to scroll up and down to see the entire list of licenses.

### NOTE

The actual image you get on the screen may differ from this example, depending on the Applications loaded on the AW Server, and their software version.

3. Copy the config.txt file to your PC or a portable storage device (e.g., a USB flash drive or a CD), so you can **Choose File** and upload all available licenses at once on the AW server.

In some occasions, it may be necessary to enter the license and the corresponding keystring of one application before you can upload all other licenses from your media (USB disk, etc..).

\*\*\*\* OR \*\*\*\*

Browse for the config.txt license file acquired from eLicense:

Manually type in the exact license string, and the exact license key.

Example License String: **VesselIQ\_Xpress**

Example License Key: **JW776XBU4EUA2J98**

**NOTICE**

The media shall be inserted into the same system as where the Service Tools is started. (i.e: If Service Tools is started on the GEHC FE laptop, insert the media in the GEHC FE laptop).

4. If not possible, manually enter the License keys delivered for your site, in the Applications corresponding fields, as shown in the example above.

Once the **Update Server** button becomes available, select it and the application(s) should populate into the “Licenses On Server” column. You might need to click in or navigate around in the *license key* field before it senses the data and activates the **UPDATE** button.

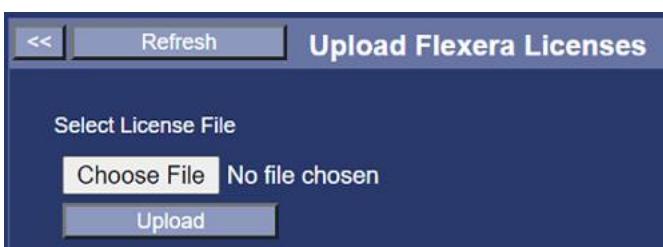
**NOTICE**

When entering the license keys, be careful about the difference between the numeral zero and the letter "O". Use a text editor application with a large font to visually verify the difference if necessary.

## 2.15.10.5 Flexera licensing

This section describes how to license the web-based AW Server Client (Web Client), and the next generation applications. These licenses are based on the License ID and are generated using FlexNet Operations (FNO).

1. The AW Server 3.2 entitlement(s) have already been created for your site in FNO. Generate the licenses file using FNO, refer to [A.3.2 Flexera Licensing on page 567](#).
2. Copy the licenses file into a portable media (USB device).
3. Insert the portable media into the Client PC or the FE laptop.
4. From the Service Tools, select **Initial Configuration > Licensing > Flexera Licensing Manager**.



5. Click on **Choose File** and select the license file.
6. To install the license file, click on **Upload**.

Register successfully! Label appears on a green background below **Upload** button.

## 2.15.11 Scalability- Clustered Servers

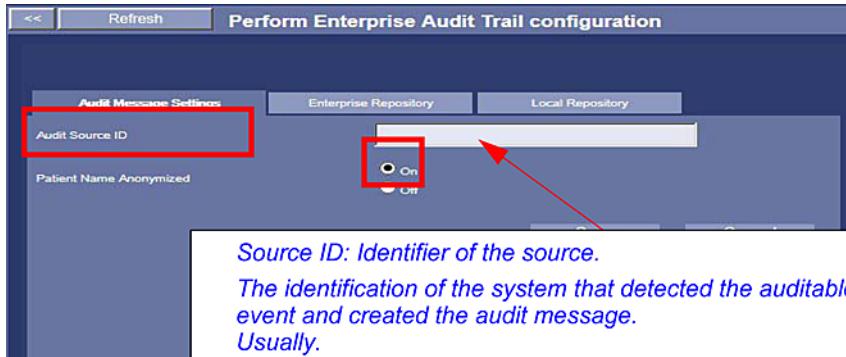
The Scalability configuration is covered by [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#).

## 2.15.12 Audit Trail (EAT)

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.

1. In *Service Tools*, select **Initial configuration > Audit Trail (EAT)**.

The *Audit Message Settings* panel displays:



2. Enter the **Audit Source ID**.

#### NOTE

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.

#### NOTE

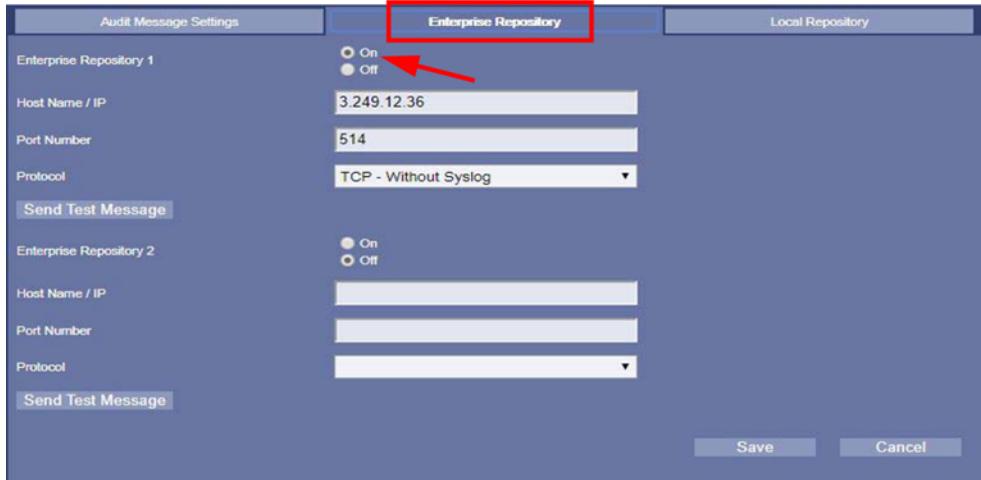
The Serial Number of the physical AW Server should be available on the chassis or in the documentation provided by the vendor.

3. Patient Name is anonymized by default.
4. Click on **Save**.
5. If your site uses an Enterprise Repository (remote log server), follow [Step 6](#) to [Step 14](#). If your site does not use an Enterprise Repository, follow [Step 15](#) to [Step 17](#).

Enterprise Repository case:

6. Click on the **Enterprise Repository** tab.

The *Enterprise Repository* panel displays:



7. Click on the **On** radio button to select Enterprise Repository.
8. Enter the Enterprise Repository network information: **Host Name / IP** and **Port Number** and select the **Protocol**. Ask the IT admin for the appropriate information.

#### 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. To enable the TLS protocol, the certificates between the AW Server and the Enterprise

Repository shall be exchanged. This will be done later through [2.18.11 Certificate Management on page 211](#).

9. Click on **Save**.
10. Make sure you are in Maintenance mode.
11. Restart all services from the *HealthPage* by clicking on the **Restart** button.

#### **NOTE**

All users are disconnected when you restart the services.

12. Exit the Maintenance mode.
13. In *Service Tools*, select **Initial configuration > Audit Trail (EAT)** and return to the *Enterprise Repository* panel.
14. To check the Enterprise Repository is alive, click on **Send Test Message**.

#### **NOTE**

If the TLS protocol is used, the check will be done later through [2.18.11 Certificate Management on page 211](#).

Local Repository case:

15. Click on the **Local Repository** tab.

The *Local Repository* panel displays:

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
110114 [2010-02-26T11:13:31] Success
110114 [2010-02-26T11:13:21] Minor Failure
110114 [2010-02-26T10:45:37] Success
110114 [2010-02-26T10:42:26] Success

**Event**

- Event Date/Time(UTC): 2010-02-26T13:35:21
- Event ID: 110114
- Event Action Code: E
- Event Outcome Indicator: 0 (Success)
- Event Type Code: 10122 (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**

- User ID: aws1.site
- User Name:
- User Is Requestor: false
- Alternate User ID:

16. Click on the **On** radio button.
17. To review an Audit Trail event, click on it.

## 2.15.13 GIB Data

This information is used to populate the Global Installed Base repository.

Perform the following steps for each piece of equipment in the AW Server system.

1. In *Service Tools*, select **Initial configuration > GIB Data**.

The *Set Global Installed Base data* panel displays:



2. Click on the **Add** button.
3. In the form that displays, fill all the fields whenever possible.
4. Click on **Apply**.
5. Repeat [Step 2](#) to [Step 4](#) for the next piece of equipment until all the equipment is documented.
6. If *Service Tools* is opened remotely from the FE laptop with access to the GE Intranet, click on **Send via PC** to send the GIB data by email.

#### **NOTE**

If you attempt to send the GIB data directly by email through the Client PC and no email account is configured, the following message displays: The email will be generated by your mail program (like Outlook).

Click on **OK** to acknowledge. When the email displays, click on the **Send** button.

7. If *Service Tools* is opened from the Client PC (usual case), use **Pull from system** to save the data first (for example, on a USB media). Access to the GE Intranet and send the data through the FE laptop.

## 2.15.14 System Hardening

#### **NOTE**

If the Secured for RMF mode is planned to be activated, then do not perform this procedure. RMF mode activation will perform different set of hardening operations.

This section describes how to enforce the security of the system, by configuring a secure log server and by enforcing the local user account password rules.

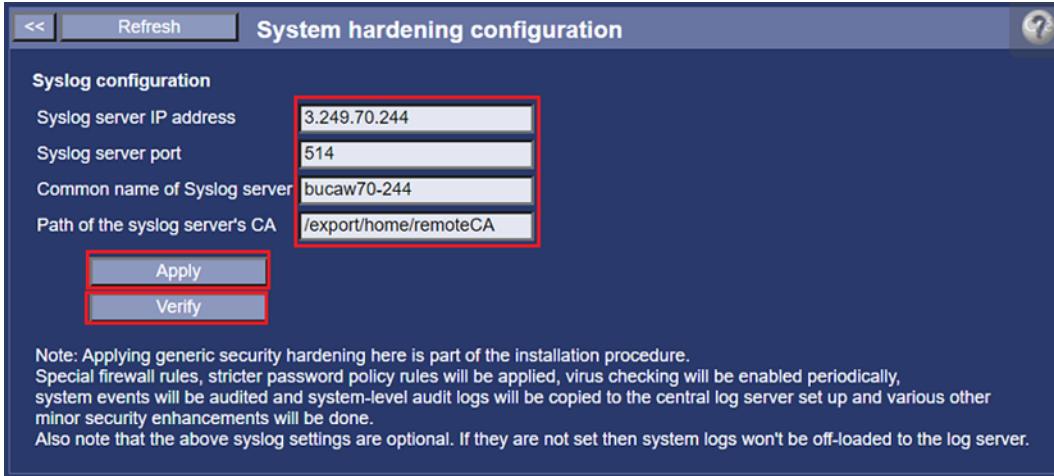
#### **NOTE**

It is **mandatory** to enforce the local user account password rules by clicking on the **Apply** button and then on the **Verify** button.

The steps to configure a secure log server are not mandatory and so the fields can remain blank. If you configure the secure log server, fill in **all** the fields, otherwise, leave **all the fields blank**.

The below steps describe how to configure a secure log server, so that the log messages generated on AW Server can be forwarded to this secure log server:

- From the Service Tools, select **Initial configuration > Hardening**.



- Copy the log server's certificate file on the local system (the AW Server):

**NOTE**

The log server can be any Rsyslog server. For instance the hospital central log server. In the below steps we will use rsyslog\_ca.crt name as the log server's certificate file name.

- Create a directory where to copy the certificate:

```
mkdir -p /export/home/remoteCA <Enter>
```

- Copy the certificate to the AW Server:

```
cd /export/home/remoteCA <Enter>
```

```
scp <log server IP>:<log server certificate> rsyslog_ca.crt <Enter>
```

- <log server IP> is the IP address of the log server.
- <log server certificate> is the path to the certificate on the log server.

I.e: `scp 3.249.70.244:/etc/pki/tls/certs/ca.crt rsyslog_ca.crt <Enter>`

- Copy the AW Server certificate file on the log server:

If the AW Server is not integrated into the log server PKI, the log server may require the AW Server certificate file. In that case, ask the local IT admin to copy the AW Server certificate file on the log server.

The AW Server certificate file is located in: /etc/pki/tls/certs/ca.crt.

- Enter the **Syslog server IP address**.

This is the IP address of the log server toward which the log messages generated on AW Server are forwarded.

- Enter the **Syslog server port**.

This is the port number of the log server.

- Enter the **Common name of Syslog server**.

This is the hostname of the log server.

The Common Name (CN), also known as the Fully Qualified Domain Name (FQDN), is the characteristic value within a Distinguished Name (DN).

Typically, it is composed of Host Domain Name and looks like for instance: www.digicert.com or digicert.com.

7. Enter the **Path of the syslog server's CA**.

This is the directory path, on the AW Server, where the log server's certificate file has been copied.

For instance: `/export/home/remoteCA`

8. Click on **Apply** button to apply the generic security hardening.

On successful completion, Hardening status is indicated in the HealthPage of Service Tools:

Hardening status	On
Hardening activation date	2022-05-04 09:39:23.633000891 +0200
Hardening verification date	N/A
<b>Refresh</b>	

9. Click on **Verify** button to verify the state of the generic security hardening.

On successful completion, Hardening status is indicated in the HealthPage of Service Tools:

Hardening status	On
Hardening activation date	2022-05-04 09:39:23.633000891 +0200
Hardening verification date	2022-05-05 11:56:54.018780409 +0200
<b>Refresh</b>	

**NOTE**

The state of the generic security hardening can be verified at any time.

**NOTE**

Refer to the Customer IT Admin to get the IP, port and common name of the log server and the server's certificate path.

To enforce the local user account password rules click on **Apply** button and then on **Verify** button.

## 2.16 Job Card IST017 - Imaging Cockpit Components Installation

The Imaging Cockpit introduces AW Server platform components that allows using a web-based AW Server Client (Web Client) to start the advanced applications.

The Imaging Cockpit is supported on the following AW Server configurations:

Tier	HW platform	Slice count license	No-Integ	Hybrid	Seamless (UV)	DICOM Direct Connect (DDC)
Physical LT	HP DL360 – G10	40k - SdC_Low_Tier_Premium	X	X		
Physical HT	HP DL360 – G10	80k - SdC_High_Tier_Standard	X	X		X
		160k - SdC_High_Tier_Premium	X	X		X
VM LT	Any	40k - SdC_Low_Tier_Premium	X	X		X (without clustering)
VM HT	Any	40k - SdC_Server_Eight_Seats	X	X		X

**NOTE**

If the Secured for RMF mode needs to be activated, then **do not perform** this procedure. Imaging Cockpit and AW Server Web client are not supported in RMF mode.

**NOTE**

The Web Client requires a license to be activated. Refer to [2.15.10.5 Flexera licensing on page 162](#).

**NOTE**

No DICOM communication is possible between Web Client and a remote DICOM host in the **192.168.x.x** IP address range.

**NOTE**

To ensure DICOM communication between the Web Client and a DICOM hosts (PACS, VNA, etc.), a dummy DICOM host shall be declared on the AW Server, and the AW Server shall be declared 3 times in the DICOM hosts. Refer to [2.18.12.2 Imaging Cockpit / AW Server Web Client on page 220](#).

The Imaging Cockpit Components are delivered either:

- In the [Physical Software Kit on page 23](#). Use the following files:

Part Number	Content	Purpose	AWS Type	Integration Mode
5872674-6  (or higher) 	aws-eml-1.12.0.iso	These iso files are used for <b>Initial Installation &amp; Upgrade/Update</b> .  They contain the Imaging Cockpit Components: <ul style="list-style-type: none"> <li>Edison Machine Light and Services</li> <li>Imaging Fabric</li> <li>Enterprise Cockpit Bundles</li> </ul>	Virtual  Physical	No-integ  Hybrid  DDC
	aws-if-1.7.2.iso			
	aws-ec-1.3.0.iso			

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use the following files to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	AWS Type	Integration Mode
5865567-5_AW_Server_Edi- son_Machine_Light_and_Serv- ices_1.12.0.zip	These compressed packages are used for <b>Initial Installation &amp; Up- grade/Update</b> .  It contains the Imaging Cockpit Components.	Virtual  Physical	No-integ  Hybrid  DDC
5865565-5_AW_Server_Imag- ing_Fabric_Component_1.7.2.zip			
5865569-5_AW_Server_Enter- prise_Cockpit_Components_ 1.3.0.zip			

**NOTE**

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

**NOTE**

The DNS setting is mandatory for the Imaging Cockpit environment. In case the site's DNS server(s) have not been set up during the early installation, they can be configured through the Service Tools, as described in [A.8.8 DNS server\(s\) setup - Alternate method on page 594](#).

## 2.16.1 Loading the Imaging Cockpit Components

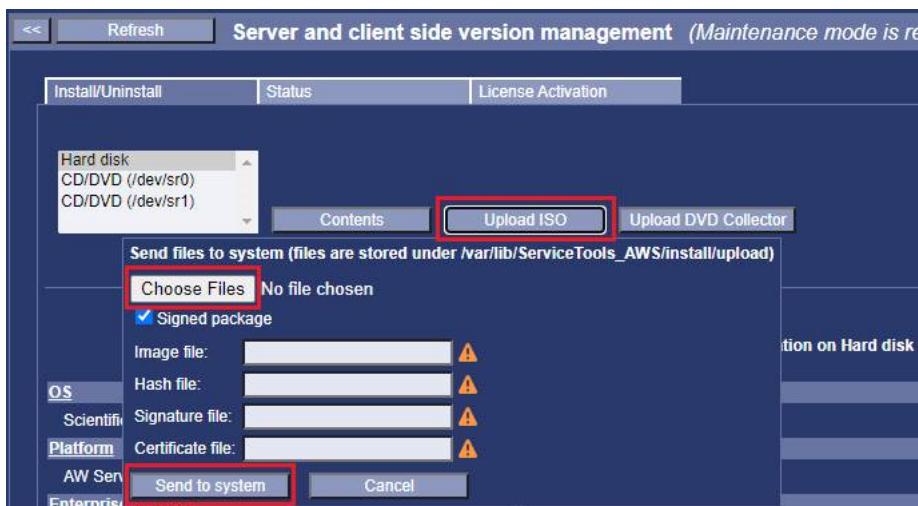
- Insert the media into the Client PC or the FE laptop.

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**.

**NOTE**

The components ISO files are signed. This means that each component 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.

5. In the pop-up window click on **Choose File** and select the component 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).



6. The **Image file** (component ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
7. To upload the ISO file click on **Send to system**.
8. Once loaded, click on **OK** in the popup that displays.
9. Verify that the component appears in the *Available for installation on Hard disk* part of the page.
10. To load the other components, proceed as in [Step 4 to Step 9](#).
11. Remove the media from the Client PC or FE laptop.

**NOTE**

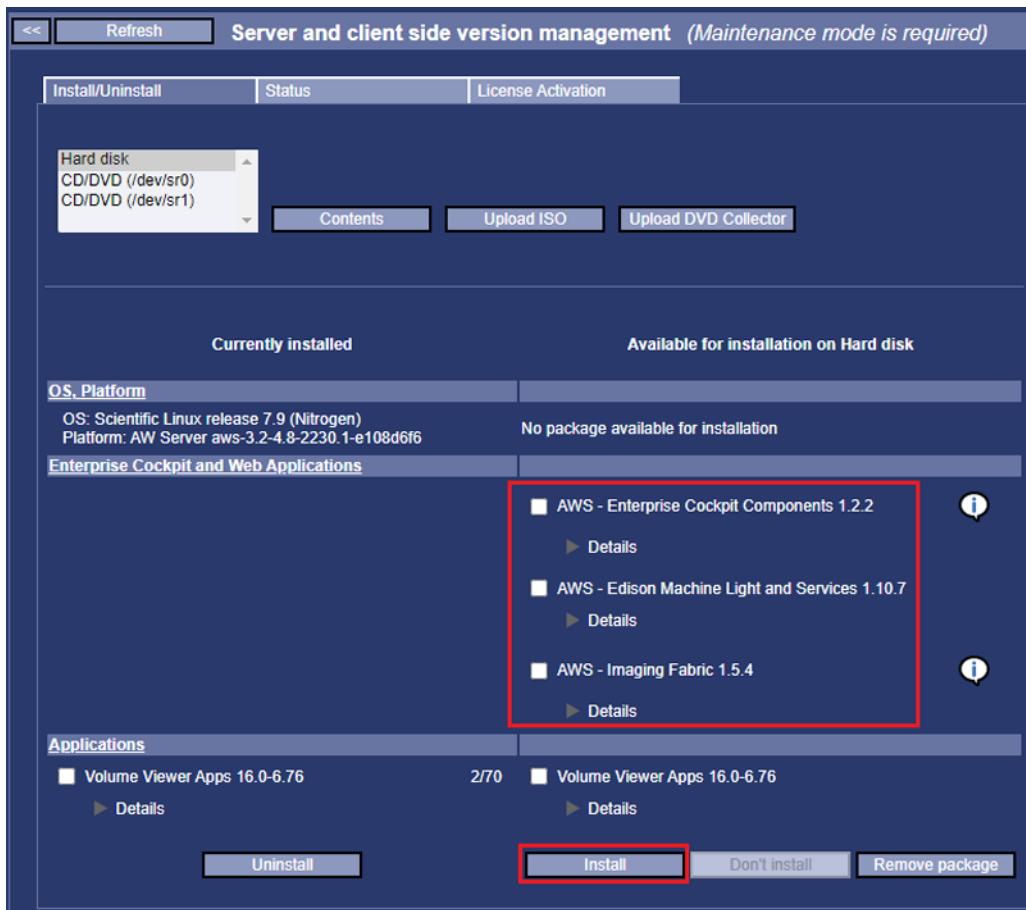
To remove a component, in the *Available for installation on Hard disk* part of the page, click to select the radio button corresponding to the component you want to remove from the AW Server hard disk and click on the **Remove package** button.

## 2.16.2 Installing the Imaging Cockpit Components

**NOTE**

Always start with the Edison Machine Light and Services component.

- Select the **Edison Machine Light and Services** component and click on **Install**.



- In the pop-up window, click on **OK** to proceed with installation.

The installation status page displays the installation steps.

#### **NOTE**

It will take several minutes to complete. Up to 10 minutes to install a component.

- When the installation is completed, click on **OK** in the window that pops up.

- Install the other components.

Proceed as in steps [Step 1](#) to [Step 3](#), to install the **Imaging Fabric** and the **Enterprise Cockpit Web Client** components.

- Select the **Install/Uninstall** tab and verify that the component(s) appears in the *Currently installed* part of the page.

6. Check now that the new items have been added to the Service Tools under **Administrative > Configuration** menu - refreshing the Service Tools may be needed before these new entries appear:



**NOTE**

To uninstall a component, in the Currently installed part of the page, click to select the radio button corresponding to the component and click on the **Uninstall** button.

### 2.16.3 Activating the Web Client

There is no specific installation package for the Web Client. The Web Client can be started from the Client PC or from the FE laptop using any web browser (refer to [1.6 Supported Web Browsers on page 27](#)).

Once licensed the Web Client needs to be activated.

**NOTE**

Before activating the Web Client, be sure that the AW Server has been rebooted after the Imaging Cockpit Components installation and before the below steps.

If not, from the Service Tools, select **Tools > Reboot** and click on **Reboot AW Server**.

1. From the Service Tools, select **Initial Configuration > Licensing > Web Client Activation**.



2. To activate the Web Client, click on **Activate**.

Once the activation is effective (it can take 10-20 minutes), the **Available** label appears on a green background next to the *Web Client status*.

**NOTE**

If the license has expired, the Web Client activation will be disabled. Refer to [2.15.10.5 Flexera licensing on page 162](#) to license the Web Client. Then, re-execute the above steps.

**NOTE**

The Web Client can be deactivated by clicking on **Deactivate**.

## 2.17 Job Card IST009 - External Application(s) Installation

### 2.17.1 Foreword

In order to address the new Quality requirement for handling safety issue with Applications running on AW Server, the following processes have been put in place.

#### 2.17.1.1 Applications delivery and installation management changes

##### 2.17.1.1.1 AW Server 3.2 Forward Production

The Advanced Applications are NO LONGER embedded in the AW Server platform software media.

- Whenever a safety issue is identified with a single Application on its dedicated SW media, it will be put "on-hold" until the issue is fixed and the new software release is ready to be put into Forward Production.
- Whenever a safety issue is identified with an Application on a multi-applications software media (i.e: Volume Viewer Apps), the multi-Apps SW media will be put on-hold and the Application impacted by the safety issue removed from the media.
- When it is done, the updated multi-Apps media will be introduced in Forward Production (without the Application impacted by the safety issue) and its package will bear a warning notice mentioning the name of the Application missing.
- When it is done, the updated AW Server platform SW media will be introduced in Forward Production (without the Application impacted by the safety issue) and its package will bear a "Product Hold" warning notice mentioning the name of the Application missing.

##### How to handle the missing Application issue:

- When installing the Applications, warn your customer about the current unavailability of the impacted application, which will become available again when the issue is corrected and the product-hold lift, through FMI delivery.

##### 2.17.1.1.2 New Application purchased and/or Applications upgrade

When a site has purchased a new Application or an upgrade (i.e: Volume Viewer applications), the Application(s) SW media is delivered.

- Whenever a safety issue is identified with a single Application on its dedicated SW media, it will be put "on-hold" until the issue is fixed and the new software release is ready to be put into Forward Production.
- Whenever a safety issue is identified with an Application on a multi-applications software media (i.e: Volume Viewer Apps), the multi-Apps SW media will be put on-hold and the Application impacted by the safety issue removed from the media.
- When it is done, the updated multi-Apps media will be introduced in Forward Production (without the Application impacted by the safety issue) and its package will bear a bear a "Product Hold" warning notice mentioning the name of the Application missing.

##### How to handle the missing Application issue:

## NOTICE

When you install the new application (of a multi-application software) purchased by the site, it will also update all applications within this package, and potentially disable an Application currently installed on the site, if this application is not contained into the new software media, because it is impacted by a safety issue.

What shall you do before installing / updating applications ?

- Identify if any application concerned by the Product Hold is installed/licensed on the system
- If yes, you need to contact your customer and ask him/her to decide whether:
  - He/she agrees that you install the new purchased Application, but this will disable an application already installed on the system (can be acceptable if the application currently installed is not regularly used by the customer) OR
  - He/she does not agree to lose temporarily the access to an application that is regularly used and prefers to postpone the new application installation and/or upgrade of applications.
- When the issue is solved and the Product hold is lift, an updated Applications package will be delivered through FMI, so you can upgrade the site with the new release.

### 2.17.1.2 Product Hold warning notice example

The following warning notice will be placed on front cover of the Applications media box jacket, whenever one or several Applications of the package would have been disabled, as containing a safety issue.



The following warning notice will be placed on back cover of the Applications media box jacket, whenever one or several Applications of the package would have been disabled, as containing a safety issue.



### 2.17.1.3 Information about registration of installed configuration

The configuration of your AW Server system and of the installed Applications MUST BE registered to the AW CCT site upon AW Server installation and configuration completion.

By sending the configuration of your AW Server system to the AW CCT web site, if it is appropriate, you will receive a configuration software key that will allow you to unlock the AW Server system and exit the Maintenance mode.

- RSvP configuration: If your AW Server is to be connected through RSvP (HCS case), it is strongly recommended to proceed with the RSvP Agent configuration and System ID (CRM Number) verification prior to installing the Advanced Applications. Doing so will allow the automatic sending of your system configuration to the AW CCT site and receiving of the configuration key.
- If your AW Server cannot be connected through RSvP (EDS case and Secured for RMF mode), the automatic sending of your system configuration to the AW CCT site and automatic receiving of the configuration key cannot be achieved. You will have to proceed with a manual registration of the configuration to the AW CCT site.

This step will have to be done once the AW Server configuration has been completed (platform, applications installation and activation, ...). Refer to [2.22.1 Configuration registration steps on page 260](#).

## 2.17.1.4 Applications Software package content

### NOTICE

Applications packages contain several media containing software and documentation. Use the appropriate media for your server type.

- Application software and docs DVD
- Application software and docs USB media

## 2.17.2 Load the Application(s) from media

### NOTICE

**Always use the latest version received for Applications.**

### Foreword

There are different ways to load the Applications from the media delivered.

Use the one applicable to your system and that better fits your needs (local / remote).

1. **Hardware servers local process**- Locally at the Server's hardware DVD drive

### NOTE

DOES NOT APPLY to Virtual AW Server loading.

- Use the standard Application SW media DVD dedicated to physical (hardware) server.
  - Insert the DVD media into the server's DVD drive
  - Proceed to section [2.17.2.1 Using the Physical server's DVD drive on page 175](#)

2. **Hardware servers remote process**- Remotely at the Client PC.

### NOTE

DOES NOT APPLY to Virtual AW Server loading.

- Use the standard Application SW media dedicated to physical server.
  - Insert the media into the client PC
  - Proceed to section [2.17.2.2 iLO DVD drive mapping - Remote loading on Physical Hardware Server on page 176](#)

3. **Virtual servers process** - Remotely at the Client PC.

Also applicable to physical hardware servers, using media dedicated to Virtual server.

- Proceed to section [2.17.2.3 Virtual server and Physical server remote loading case on page 177](#).

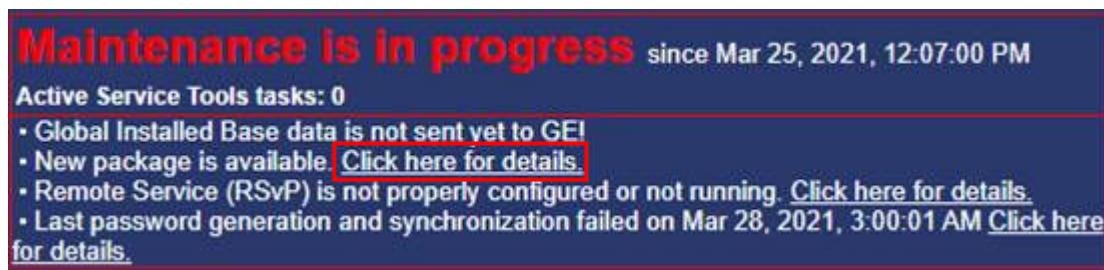
**NOTE**

Section [2.17.2.4 Loading Advanced Applications from USB device - eDelivery on page 178](#) gives an alternate method to load using the File transfer tool.

#### 4. Loading from electronic files

When loading from electronic files, always refer to **5761599-8EN: AW eDelivery Service Guide** for detailed instructions.

- For the systems connected via RSvP, if new Application(s) are available, they have been automatically loaded onto the AW server. 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 Install the Application, refer to [2.17.3 Install the Application\(s\) on page 178](#).

### 2.17.2.1 Using the Physical server's DVD drive

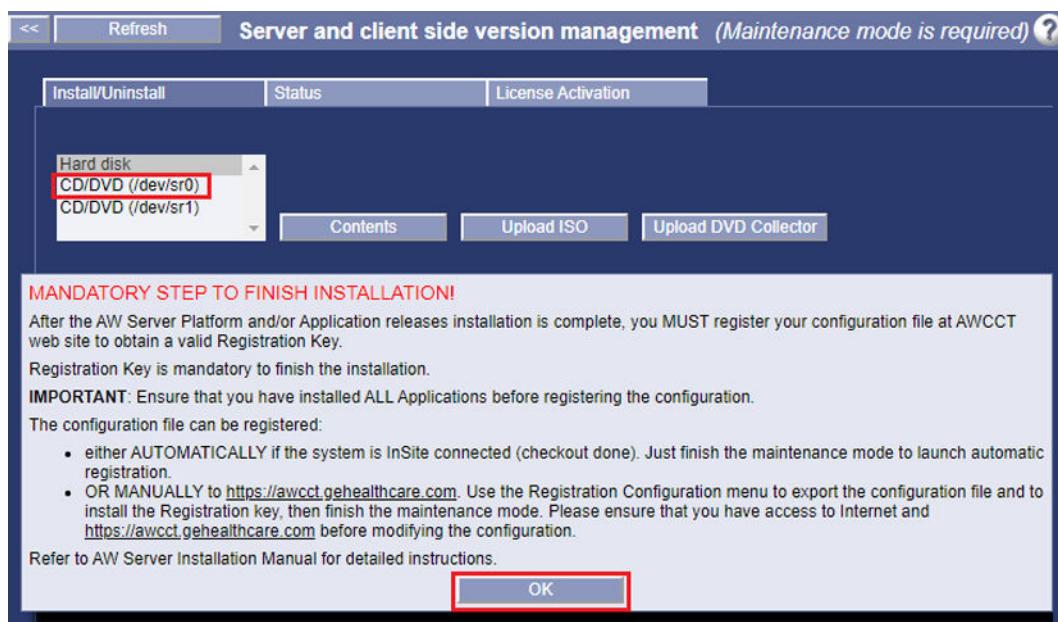
Use the standard Application SW media DVD dedicated to physical (hardware) server.

- At the physical server hardware:**

Insert now the Application DVD media you want to install into the Server's DVD drive.

- At the Client PC or FE laptop:**

Launch the **Version Management** tool under **Maintenance** sub-menu.



Carefully read the warning message and make sure you understand it prior to click on **OK** button to close the message.

3. Make sure the *Install/Uninstall* tab is selected or select it.

Wait for a few seconds for the media to be mounted, then select **CD/DVD (/dev/sr0)** and click on **Contents** (DVD drive of the server hardware).

The "Available for installation on Hard disk" section will get populated with the new package available for installation. Make sure the version you are about to install is appropriate (I.e: Version is not older than the one currently installed - upgrade case).

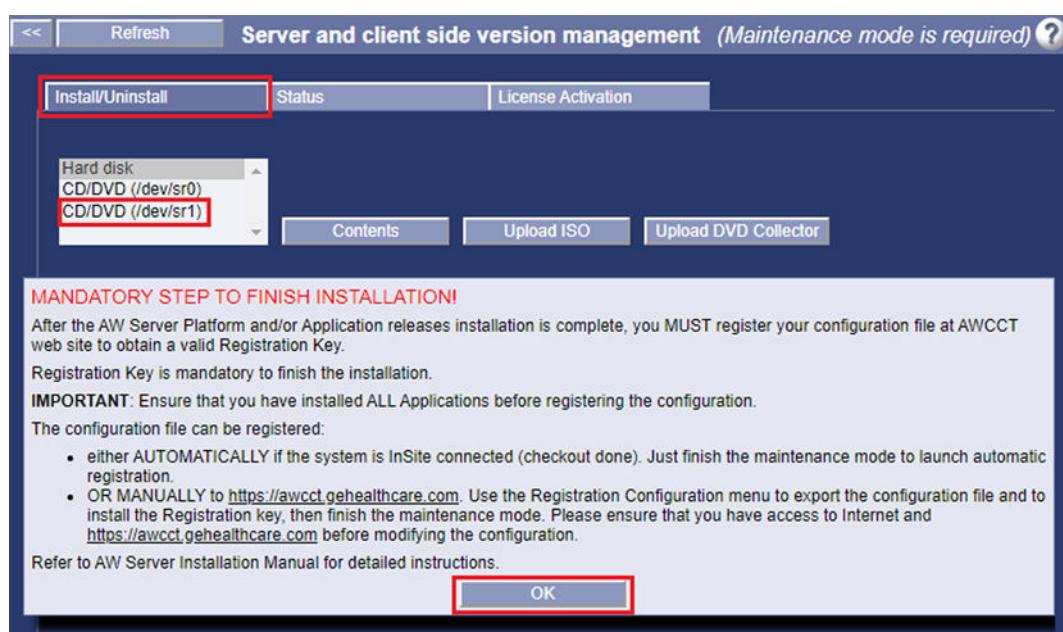
4. Install the Application now. Goto [2.17.3 Install the Application\(s\) on page 178](#).

## 2.17.2.2 iLO DVD drive mapping - Remote loading on Physical Hardware Server

Loading Applications software from the Application SW media can be done at the Client PC, if you map the Client media via the iLO Service Processor.

Use the standard Application SW media applicable to your system.

1. **At the Client PC or FE laptop:** Insert now the Application media you want to install into the Client PC's.
2. Refer to [A.6 Software Loading Through iLO on page 579](#) for details on iLO UI startup and mapping a media drive.
  - a. Open a web browser and launch the iLO interface: `http://<iLO_IP_address>`.
  - b. Login as **root**.
  - c. Start the "Console redirection".
  - d. Map the media drive of the Client PC.
3. Under the Service Tools / Maintenance menu:
  - a. Launch the **Version Management** tool under **Maintenance** sub-menu.



## NOTICE

Carefully read the warning message and make sure you understand it prior to click on OK button to close the message.

- b. Make sure the **Install/Uninstall** tab is selected or select it.
- c. Wait for a few seconds for the media to be mounted, then select **CD/DVD (dev/sr1)** and click on **Contents** (media drive of the server hardware).
4. The "Available for installation on Hard disk" section will get populated with the new package available for installation. Make sure the version you are about to install is appropriate (i.e: Version is not older than the one currently installed - upgrade case).

Install the Application now. Go to [2.17.3 Install the Application\(s\) on page 178](#)

### 2.17.2.3 Virtual server and Physical server remote loading case

The following procedure shall be used to load Applications remotely from the PC for a Virtual AW Server and/or a Physical AW Server if the servers room is not accessible. In this case, prepare Applications loading through the iLO of your server (refer to procedure in [A.6 Software Loading Through iLO on page 579](#)).

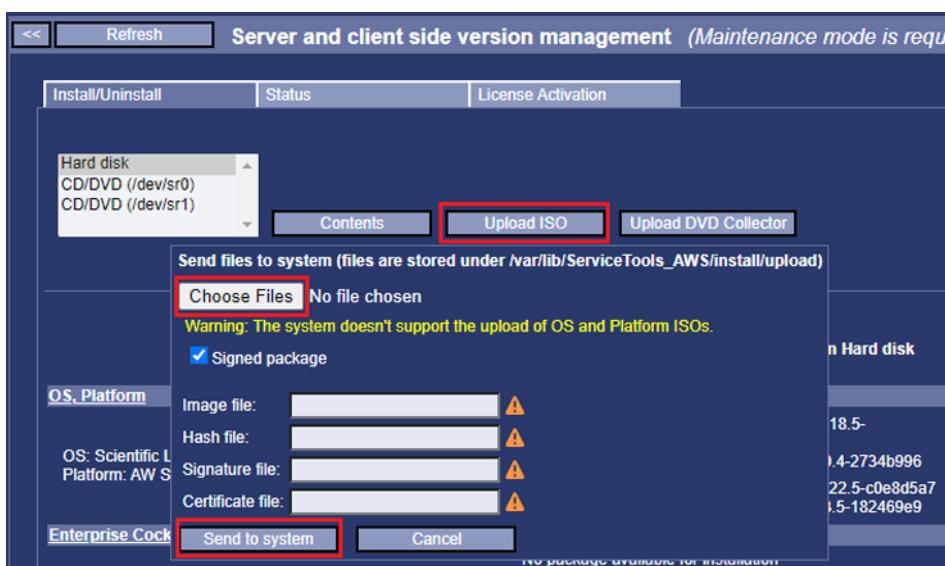
1. Insert the Application Media into the Client PC or the FE laptop.
2. From the Service Tools, select **Maintenance > Version Management**.
3. Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message.
4. Click on **Upload ISO**.
5. If the application 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.

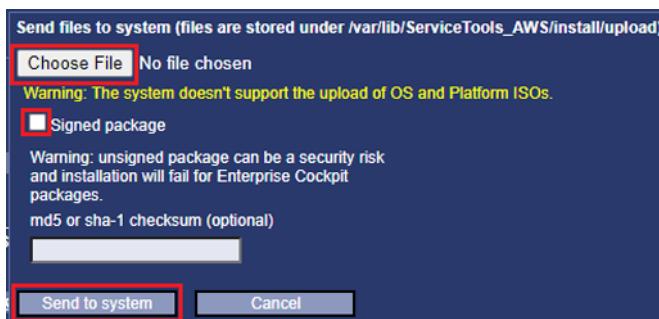
If the Secured for RMF mode is planned to be activated, only signed ISO is accepted.

- a. In the pop-up window click on **Choose File** and select the 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).



- b. The **Image file** (component ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.

6. If the application ISO file is not signed, follow the below substeps.
  - a. In the pop-up window, uncheck the **Signed package** check box.
  - b. Click on **Choose File** and select the ISO file stored on the media.



- c. 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.
7. To upload the ISO file click on **Send to system**.
8. When the file is loaded, click on **OK** in the pop-up window.
9. Verify that the ISO file appears in the *Available for installation on Hard disk* part of the page.
10. Remove the media from the Client PC or FE laptop.
11. Install the Application.

Proceed to [2.17.3 Install the Application\(s\) on page 178](#).

## 2.17.2.4 Loading Advanced Applications from USB device - eDelivery

eDelivery is a new delivery method which allows to provide AW application products as electronic files. The electronic files are manually downloaded from a download server and installed through USB device.

### NOTE

At the time of release of this manual, eDelivery process may not be fully available for all AW applications. Refer to eDelivery process documentation for details.

### NOTE

Verify that the USB file system is supported in eDelivery, before installing applications from USB device.

The list of applications supporting eDelivery process will be regularly communicated.

You will also be able to refer to [AWeDelivery Service Guide 5761599-8EN / DOC1888559](#) for detailed instructions about:

- Connection to eDelivery server and download of application digital kit.
- Application loading from USB device using *Version Management* (refer to section [2.17.2.3 Virtual server and Physical server remote loading case on page 177](#)).
- Demo exams loading from USB device.
- Troubleshooting.

## 2.17.3 Install the Application(s)

See [2.17.5 Applications Profile on page 182](#) for the list of supported Applications.

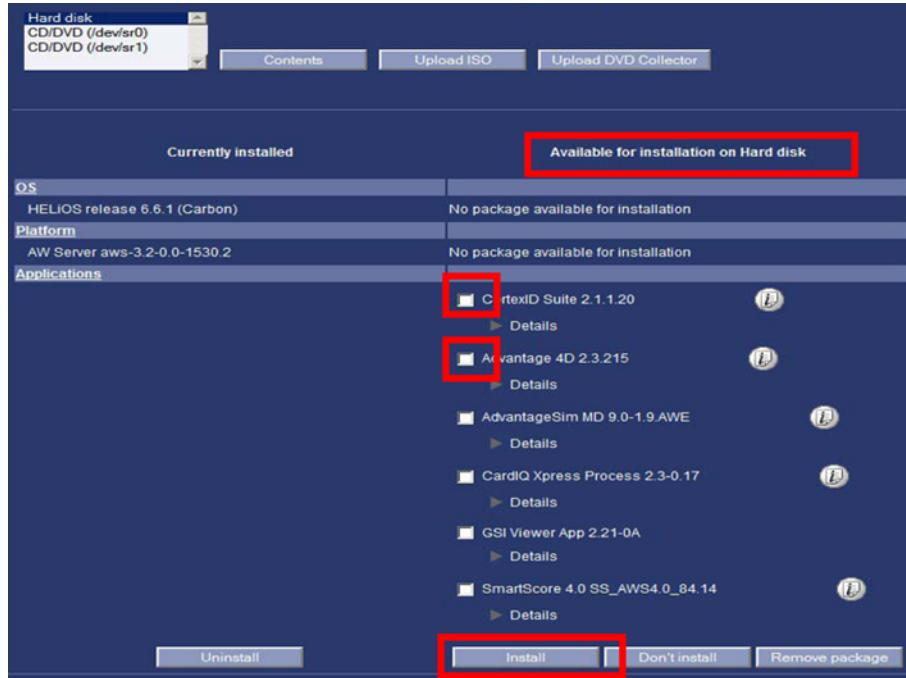
### NOTE

Do not install the applications for which no license has been ordered/purchased by the customer.

**NOTE**

There is an installation conflict between CardIQ Xpress Process and Advantage SIM MD. If both CardIQ Xpress Process and Advantage SIM MD need to be installed, install CardIQ Xpress Process package first, then install Advantage SIM MD.

1. Use the Version Management tool to select and install the Applications loaded in [2.17.2 Load the Application\(s\) from media on page 174](#).



Applications will not show up in the "Available for installation on hard disk" until they have been loaded from their media.

**NOTE**

For the systems connected via RSvP, if new applications versions are available, they have 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.

2. After successful completion of Applications software loading, the "Available for installation on Hard disk" section gets populated with the new package available for installation.
  - Make sure the version you are about to install is appropriate (I.e: Version is not older than the one currently installed - upgrade case).
  - Click the radio button to select the Application(s) for installation.

**NOTE**

You can select several applications to be installed one after one in the same shot.

- Click on the **Install** button. The Application(s) start(s) loading.

3. Acknowledge the information message by clicking on **OK**.

- *Do you really want to install the following packages:*

*Appl 1*

*Appl 2*

*Appl n*

It takes time to extract and install the packages. Please be patient. When the Application(s) is (are) loaded, a message will say so and they will appear in the "Currently installed" section.

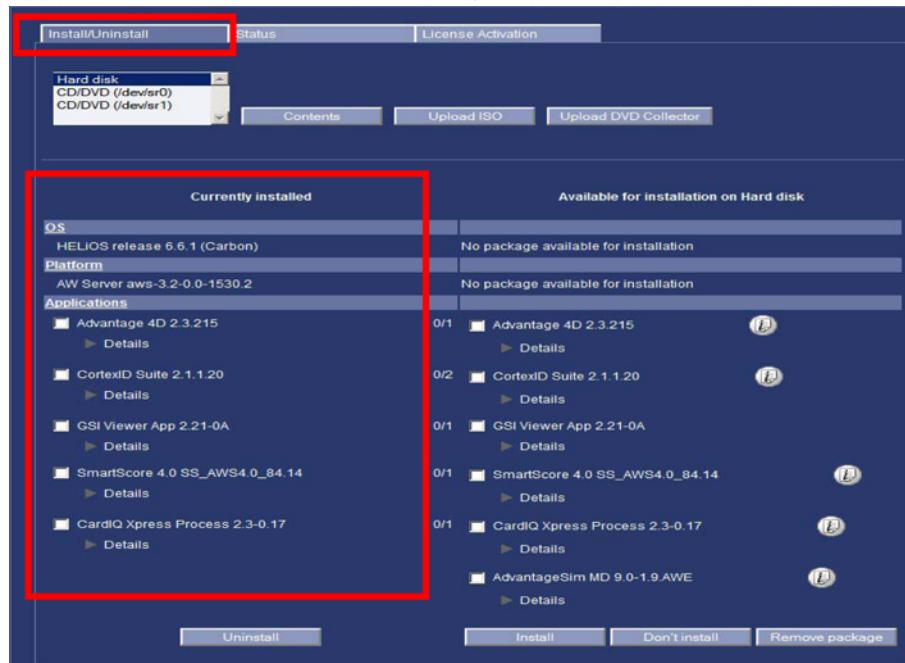
When done, proceed with the next Application(s) installation.

### NOTICE

**Pre-requisite for CardIQ Xpress Process v2.3 installation:** Volume Viewer, CardIQ Xpress Reveal and Pre-processing must be licensed and installed. CXP license must also be set before installing the CXP package.

4. When done, the *Install/Uninstall finished successfully* message displays.
  - Click on **OK** to acknowledge the message.
  - Select again the **Install/uninstall** tab.

Application now show in the "Currently installed" section as in the example below:



5. If you have installed the *Advantage SIM* and/or *Advantage 4D* application(s), check now that new menus have been added to the service tools under the **Maintenance** menu - You may need to refresh the service tools before these new entries appear:



6. If you have installed the ZFP application (next generation application), check now that a new menu has been added to the Service Tools under **Administrative** menu - You may need to refresh the service tools before these new entries appear:



#### **NOTE**

##### **Informational step: Application uninstallation:**

- To uninstall an application, click to select the radio button corresponding to the application and click on the **Uninstall** button.
- To remove a package, click to select the radio button corresponding to the package you want to remove from the AW Server hard disk and click on the **Remove package** button..

## **2.17.4 Activate the Application(s)**

#### **NOTE**

For next generation applications there is no activation.

Make sure the applications are licensed prior to activate them. Refer to [2.15.10.4 Floating License – Application licensing on page 160](#).

Applications shall be activated in order to be available once they have been licensed and installed.

They can be de-activated if necessary, for instance when an application shall not be left running on site.

Applications are not activated by default. Make sure to perform the following steps to activate applications. This is also necessary when upgrading from AWS2.0 release.

#### **NOTE**

Only activated licenses and the related applications are listed (shortcuts are filtered out) in the configuration file.

1. Click on the **License Activation** tab.

The following menu (example) displays:

Server and client side version management (Maintenance mode is required)					
Install/Uninstall		Status		License Activation	
Refresh		Select available		Apply	
Activated	Application Name	Licensed	Key String	License Information	Application Version
<input checked="" type="checkbox"/>	3D Viewer	Volume_Viewer	NFVB9DR115TT6CD	12.3-4.151	
<input type="checkbox"/>	Advantage CTC	CT_Colono_Pro3D_EC	NS7U29DYMNYNENR4	12.3-4.151	
<input type="checkbox"/>	Autobone	AutoBone_Xpress	TF9L8MLVZSXZ6PU9	12.3-4.151	
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_MultiOrgan	J8T926AC88CZS8VA	12.3-4.151	
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Neuro	2ADAFPKJF9YSKYWE	12.3-4.151	
<input type="checkbox"/>	CardIQ Function	CardIQ_Function_Xpress	7D78F4D4M4QZBHJN	12.3-4.151	
<input type="checkbox"/>	CardIQ Fusion PET	CardIQ_Fusion_PET	WT88WRU4V6DQ26NC	12.3-4.151	
<input type="checkbox"/>	CardIQ Fusion SPECT	CardIQ_Fusion_SPECT	KWAEXSCODEBTAEG9	12.3-4.151	
<input type="checkbox"/>	CardIQ Xpress	CardIQ_Xpress_Elite	G23H8C2YQKL949AM	12.3-4.151	
<input type="checkbox"/>	CardIQ Xpress	CardIQ_Xpress_Reveal	QKXV4PU3TBX34SBF	12.3-4.151	
<input type="checkbox"/>	Colon VCAR	Colon_VCAR_EC	MT284AT2FHJKXYZN	12.3-4.151	
<input type="checkbox"/>	Dynamic Shuttle	Dynamic_Shuttle	VY9LQ324NZ7DST24	12.3-4.151	
<input type="checkbox"/>	FlightPlan for EVAR A	FlightPlan_for_EVAR_A	- Not licensed -	12.3-4.151	
<input type="checkbox"/>	FlightPlan for EVAR CT	FlightPlan_for_EVAR_CT	UTSAW87BNE9J29HD	12.3-4.151	
<input type="checkbox"/>	FlightPlan for EVAR MR	FlightPlan_for_EVAR_MR	BKGFYQH368R6M62T	12.3-4.151	
<input type="checkbox"/>	FlightPlan for Liver	FlightPlan_for_Liver	BDYUXM7GC6QUB7AR	12.3-4.151	
<input type="checkbox"/>	GSI MSI	GSI_MSI	YH9S83UGH2U24Q2M	12.3-4.151	
<input checked="" type="checkbox"/>	GSI Viewer	GSI_Viewer	C6ESBOWYZJL2FHS4	2.20-04	
<input type="checkbox"/>	GSI Volume Viewer	GSI_Volume_Viewer	DD6EHUH38QNMWWA8	12.3-4.151	

2. Scroll down to see all listed applications.
3. Click on **Select available** button to automatically check the boxes of all licensed application available on the Floating License Server **OR** select the Application(s) to be activated.  
Also make sure to uncheck all licensed Applications that are should not be activated.
4. Click on **Apply** when done. You may also have to click on the **Refresh** button to display.

#### NOTE

##### License Information column:

- Not licensed - There is no license available for the application.
- A license is displayed - There is a Floating license available for the application.

##### Application Name column:

Not installed - You need to load the Application first from its media.

#### NOTE

"Conf" output lists the applications which has at least one activated license. Only the activated licenses are listed.

## 2.17.5 Applications Profile

Applications currently supported with the AW Server 3.2 release are:

### 2.17.5.1 Volume Viewer applications

#### NOTE

Unlike earlier versions of Volume Viewer Applications 11.x for AW Server 2.0 platform, the basic Volume Viewer application 12.3 (or up) or the Volume Viewer application 13.0

(or up) needs a license key to be enabled for AW Server 3.2. The AW Server 3.2 platform license key does not include the Volume Viewer license.

The Volume Viewer license is required as a pre-requisite to launch all other Volume Viewer Applications.

All Volume Viewer Applications use the same logfile: **Voxtool.log**.

All Volume Viewer Applications use Floating license mode, except AutoLaunch (pre-processing) which uses Node-Locked license mode.

#### **NOTE**

Refer to the Volume Viewer Applications Service Note (SNAW3090) and to the Applications dedicated RMF to get the supported Applications and Integration Mode(s).

#### **NOTE**

All the Volume Viewer Applications in release 12.X / 13.X (or up) are compatible with single and dual monitor configurations.

Whenever there is an Installation Manual and/or a ReadMeFirst document delivered with the application (e.g: VV 12.3, CardIQ Xpress Process, etc..), refer to the supplied document for more details.

## **2.17.5.2 Other Applications supported**

#### **NOTE**

Whenever there is an Installation Manual and/or a ReadMeFirst document delivered with the application, refer to the supplied document for more details.

Application Name in Version Management	Application version	License Modes supported	License Keystring	legacy keystring supported	Shortcuts (in AW Server client desktop)	AW Logfile name
CardIQ Xpress Process	2.3 Ext. 6 (or up)	Floating	CardIQ_Xpress_Process Prerequisites: Volume_Viewer CardIQ_Xpress_Reveal AutoLaunch	N/A	N/A (launched via CardIQ Xpress Reveal or via AutoLaunch)	cardiqprocess.log
CortexID Suite	2.1 Ext. 6 (or up)	Floating	CortexID_Suite	N/A	CortexID Suite	cortexidsuitelog
CortexID Suite PIB	2.1 Ext. 6 (or up)	Floating	CortexID_Suite_PIB	N/A	CortexID Suite	cortexidsuitelog
SmartScore 4.0	4.0 Ext. 200 (or up)	Floating	SmartScore_40	N/A	SmartScore 4.0	sscorelog
GSI Viewer	2.2 Ext. 5 (or up)	Floating	GSI_Viewer	N/A	GSI Viewer GSI Curved GSI General...	gsiviewerlog
Advantage 4D	2.3 Ext. 5 (or up)	Floating	Advantage_4D_CT	N/A	Advantage 4D	See Advantage 4D manual

AdvantageSim MD	9.0 Ext. 4 (or up)	Floating	AdvantageSim SimMD_MultMod4D SimMD_Opt_CT_AtlasRePlan SimMD_Opt_MR_PelvisSeg	N/A	AdvantageSim MD	See Advantage-Sim MD manual
Quantib Brain	1.2 (or up)	Floating	Quantib_Brain	N/A	N/A	See Quantib Brain manual
CVI42_CMRA42	5.3 Ext. 4 (or up)	Floating	cvi42_cmra42 cvi42_mitral	N/A	CVI42_CMRA42	See cvi42 manual

Pre-requisite for **CardIQ Xpress Process (CXP)** installation:

- Volume Viewer, CardIQ Xpress Reveal and Pre-processing must be licensed and installed.
- CXP license must also be set before installing the CXP package.

Applications installation and configuration is complete

**Proceed to** [2.18 Job Card IST010 - Administrative Configuration on page 184](#)

## 2.18 Job Card IST010 - Administrative Configuration

1. From the Service Tools menu, click on **Administrative** to expand the menu.
2. From the Administrative menu, click on **Configuration** to expand the menu.



### 2.18.1 Configuring DICOM hosts in Service Tools

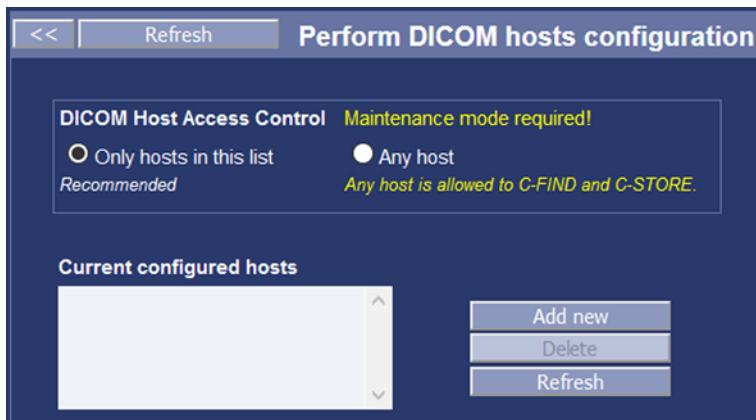
The following procedure describes how to configure one or more DICOM hosts to allow data exchange between them and the AW Server.

#### NOTE

For Seamless integration, the only necessary DICOM host declaration is the Universal Viewer PACS server. The DICOM port of the Universal Viewer is 104.

1. Get the DICOM hosts information from the IT Admin.
2. In Service Tools, select **Administrative > Configuration > DICOM Hosts**.

The *Perform DICOM hosts configuration* interface appears.



3. Select a **DICOM Host Access Control** feature:

- **Any host** if you want to allow any DICOM host to perform C-FIND and C-STORE.
- **Only hosts in this list** if you want to allow just the ones in the DICOM host list.

Default setting recommended is **Only hosts in this list**. This procedure must be performed in Maintenance mode, otherwise it's greyed out and not be able to change it. The function automatically restarts Nuevo in a few seconds after the setting was changed.

**NOTE**

This feature is not enabled in Seamless and DDC integration modes.

4. Click on **Add new**.

The *DICOM hosts configuration* page appears.

5. Fill all mandatory fields (marked with an asterisk(\*)) to configure a host. Other fields are optional.

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

**NOTE**

The DICOM Hosts file is part of Nuevo.

The file is `/export/home/sdc/nuevo/resources/network/network-cfg.xml`.

**DICOM Direct Connect integration mode only**

Preferred compression format	Automatic	Select Automatic (default). If image data loading is slow, select the compression used by this DICOM host to store the images. Wrong selection can degrade the image data loading speed.
Allow speed-up of C-FIND query	Multi-value UIDs for C-FIND	Select Multi-value UIDs for C-FIND (default) to speed-up application launch. Select Relational C-FIND if supported by this DICOM host or None if application launch fails.
Allow early response for C-STORE	<input checked="" type="checkbox"/>	Speeds up retrieval of the images, turn it off if application launch fails.
C-MOVE query strategy	Synchronous single UID	Use default value unless otherwise instructed
C-MOVE instance level threshold	4	Use default value unless otherwise instructed
C-FIND cancellation strategy	SyncSendCancel	Use default value unless otherwise instructed

**Apply**    **Cancel**

- Check the **Encrypted (TLS)** checkbox to exchange data in secure mode.

#### NOTE

In this case the certificates shall be exchanged between the AW Server and the DICOM Host. Refer to [2.18.11 Certificate Management on page 211](#).

#### NOTE

If the Secured for RMF mode needs to be activated, then make sure that the configuration is set to secure connections (TLS) to the required DICOM host. Please also note that FE can configure exceptions for DICOM sources which do not support TLS after the Secured for RMF activation. See details in [2.31.3.4 Interoperability with non-RMF compliant systems on page 462](#).

Checking the **Encrypted (TLS)** checkbox sets the **Port** to 2762. The AW Server declaration on DICOM images sources should also use the port 2762.

- If you didn't check **Encrypted (TLS)**, set the **Port** to:

- 4006** for AW Server DICOM
- 104** for Universal Viewer and Enterprise Archive DICOM

- To check if the host is reachable:

- Click the **Check address** button to test the address of the host with a standard ping.

- b. Click the **Check DICOM** button to perform a DICOM ping.

**NOTE**

If the **Encrypted (TLS)** checkbox is checked, the certificates shall be exchanged between the AW Server and the DICOM Host. Refer to [2.18.11 Certificate Management on page 211](#).

9. Check **Custom Search** to enable this option and prevent the PQCS/VNQ from querying the whole database. Otherwise, the query may fail due to the high amount of data.

**10. NOTE**

The C-FIND tags are used when NUEVO sends C-FIND commands to the remote host in order to build the Remote Worklist in NoInteg, Hybrid or DDC integration mode.

Check or uncheck the box(es) to enable or disable the two optional DICOM tags: **Institution** and **Reading Physician**.

**NOTE**

By default, they are disabled, because, according the IHE standard, remote hosts are not “required” to support them, but many host do (e.g. EA, AWS).

The other C-FIND tags cannot be changed from Service Tools, because, according the IHE standard, remote hosts are “required” to support them. However, if it is really necessary, they can be changed to `false` in the appropriate section in the `network-cfg.xml` configuration file. This configuration file is located in `/export/home/sdc/nuevo/resources/network/network-cfg.xml`. Every DICOM host has a "node" tag structure in the configuration file.

11. To enable the PACS/VNA supporting Storage Commitment:

- a. Check the **Storage Commitment Supported** option.
- b. Fill out the **SC host name**, **SC AE title**, **SC IP address** and **SC port**.

12. Check the following options to enable them:

- **Allow query**: allows the remote DICOM host to query the AW Server
- **Allow retrieve**: allows the remote DICOM host to retrieve from the AW Server
- **Allow store**: allows the remote DICOM host to store to the AW Server

13. If applicable, add **Comments** for the FE or IT Admin.

14. In case of front-end integration in DDC or Hybrid mode, enter the **Authentication URL** to authenticate token-based login.

15. In case of DICOM Direct Connect integration:

- a. Check which compression mode the PACS/VNA supports and select one of the following **Preferred compression format**:

- **Automatic** (default)
- **JPEG Lossless**
- **JPEG 2000 Lossless only**
- **RLE**
- **Uncompressed**

- b. Check if the PACS/VNA supports **Relational C-FIND** or **Multi-value C-FIND** and select one of the following in the **Allow speed-up of C-FIND query** field:

- **Relational C-FIND**
- **Multi-values UIDs for C-FIND** (default)
- **None**

- c. If applicable, check the **Allow early response for C-STORE** option.  
Checking this option speeds up retrieval of images.
- 16. Click **Apply** to complete the host configuration.
- 17. Proceed to the next DICOM host configuration.

**NOTE**

All configured DICOM hosts can be saved when the **Maintenance > Backup** tool is run, and correspondingly restored when the **Maintenance > Restore** tool is run.

## 2.18.2 Configuring DICOM Printers and Filmers

**This feature is not available with Seamless integration and Secured for RMF mode.**

1. • From the Service Tools menu, click on **Administrative > Configuration > DICOM Printers**. The "Perform DICOM printers configuration" interface displays.



- Ask your customer what hospital name shall be displayed on the films.

Use only the ISO-8859-1 English character set for DICOM printer configuration. Other character sets are not supported. If you do not enter the Hospital name for Filmer, you will not be authorized to setup the DICOM printer parameters.

1. • Enter the Hospital name for Filmer and click on Apply button
2. • Click on Add button  
The "Perform DICOM printers configuration" interface expands.

**Perform DICOM printers configuration**

Basic English character set shall be used. See Administrator Guide for details!

Hospital name for Filmer \* BUC AW LAB | Apply

**Current configured DICOM printers**

PRINT_SCOP	Add
	Delete
	Refresh

Label\*   
 Host name\*   
 Application Entity Title\*   
 IP address\*   
  
 Port\*

Layouts \*


3. All mandatory fields (the ones marked with an asterisk(\*)) must be filled out to configure a printer or a filer. Other fields are optional.

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

Following the rules and limitations, enter or select all available information for the printer.

Do these steps for each DICOM printer or filer to be added.

4.
  - Enter the first set of parameters as specified by the IT admin or the printer Vendor FE (Label, Hostname, AE Title, IP address, Port, and Layouts).
  - You can check that the Printer is alive by clicking on the **Check IP** button then check that the AE Title and the Port are OK by clicking on the **Check DICOM** button.
5.
  - Scroll down to access the next set of parameters
  - Enter the next set of parameters as specified by the IT admin or the printer Vendor FE.

Film size *		Width		Height		Width		Height	
<input type="checkbox"/>	8in x 10in					<input type="checkbox"/>	14in x 17in		
<input type="checkbox"/>	8.5 x 11in					<input type="checkbox"/>	24cm x 24cm		
<input type="checkbox"/>	10in x 12in					<input type="checkbox"/>	24cm x 30cm		
<input type="checkbox"/>	10in x 14in					<input type="checkbox"/>	A4		
<input type="checkbox"/>	11in x 14in					<input type="checkbox"/>	A3		
<input type="checkbox"/>	11in x 17in					<input type="checkbox"/>	A		
<input type="checkbox"/>	14in x 14in								

Filming mode  True Size

Printer pixel size  micron

Density  -1 Min  -1 Max

Magnification type  CUBIC

Smoothing factor\*

Trim

12 bits image supported

Color supported

Memory  20 MBytes

Configuration information

\* Mandatory fields

6. • When done, click the **Apply** button.
7. • Proceed with the next printer declaration.

## 2.18.3 Configuring PostScript Printers

This feature is not available with Seamless integration and Secured for RMF mode.

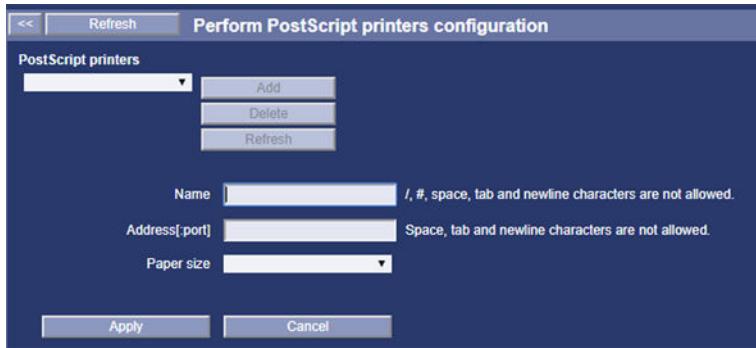
1. • From the Service Tools menu, click on **Administrative > Configuration > PostScript Printers**.

The "Perform PostScript printers configuration" interface displays.

PostScript printers		Perform PostScript printers configuration		
<input type="button" value="&lt;&lt;"/>	<input type="button" value="Refresh"/>	<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Refresh"/>
<input style="width: 150px; height: 20px; border: 1px solid black; padding: 2px; margin-bottom: 5px;" type="button" value="Printer1"/> <input style="width: 100px; height: 20px; border: 1px solid black; padding: 2px;" type="button" value="Add"/> <input style="width: 100px; height: 20px; border: 1px solid black; padding: 2px;" type="button" value="Delete"/> <input style="width: 100px; height: 20px; border: 1px solid black; padding: 2px;" type="button" value="Refresh"/>				

2. • Click on **Add** button

The "Perform PostScript printers configuration" interface expands.



3. Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

Following the rules and limitations, enter all available information for the printer. Note that all fields are mandatory.

Do these steps for each PostScript printer to be added.

4. • Enter the parameters as specified by the IT admin or the printer Vendor FE (Name, IP Address, Port, and Paper size).
5. • When done, click the **Apply** button.
6. • Proceed with the next printer declaration.

## 2.18.4 Users (EA3) (User account configuration)

Follow the guidelines hereafter to manage the Service, Admin and/or Standard users.

For Full or Seamless Integration with the PACS, Client Users are defined at the Universal Viewer level, not at the AW Server level so you can bypass the following steps.

### **NOTICE**

EA3 configuration page may not be properly working in some web browsers. Refer to [1.6 Supported Web Browsers on page 27](#).

The USER ACCOUNT configuration utility is used to create and modify user accounts, server information for an existing enterprise user account network, establish groups for the user accounts, and assign levels of access or roles for the user groups.

**There are TWO ways to establish user accounts:**

- Local user accounts
- Active Directory or enterprise user accounts

The site IT administrator should make this decision. Use only one method or the other, NOT both, to avoid potential group permission conflicts and unnecessary administrative complexity.

You will now create two local accounts, including one account for the site IT administrator.

### **NOTE**

Involve the site IT admin when setting up local user or enterprise accounts, since they will administer these accounts after system handoff.

- If the site IT admin wants to use local user accounts, perform the “**Local User Account Configuration**” procedure.
- If the admin wants to use Enterprise user accounts, perform the “**Enterprise User Account Configuration**” procedure.

- If the Secured for RMF mode is planned to be activated, then perform the “**Enterprise User Account Configuration**” procedure. (If for some reason this is not possible, then create the local users only after the RMF mode activation. Refer to [2.31.3.3 Finalizing configuration after Secured for RMF Mode activation on page 461](#)).

Do NOT perform both procedures.

- Click on **Users (EA3)**.

The “Perform Enterprise Authentication, Authorization and Audit configuration” page will display at the Local Users tab.

Local Users		Groups	Enterprise																
<a href="#">Add Local User</a>																			
Max Logon Attempts Before Lock	5																		
Lock Duration (Minutes)	15																		
<b>Password rules:</b>																			
• Minimum Password Length	8	[ 6 - 63 ]																	
• Maximum Password Length	63	[ 14 - 63 ]																	
• Minimum Password Retention Period	1	[ 0 - 1 ]																	
• Password Expiry Period	90	[ 1 - 1024 ]																	
• Password Expiration Period for Admin	1024	[ 1 - 1024 ]																	
• Previous Password Count	10	[ 1 - 32 ]																	
• Your password cannot include your Logon Name, cannot be a palindrome, or be easily guessed.																			
<input checked="" type="checkbox"/> Advanced Password Rules: Your password must contain 1 number, 1 uppercase, 1 lower case, and 1 non-alphanumeric character and cannot contain 3 consecutive same characters or a whitespace character.																			
<a href="#">Apply Configuration</a> <a href="#">Restore Configuration</a>																			
<b>Local Users</b> <table border="1"> <tr> <td>admin</td> <td>Username</td> <td>admin</td> <td>Change Password</td> </tr> <tr> <td>limited</td> <td>Full Name</td> <td></td> <td>Change Name</td> </tr> <tr> <td>service</td> <td></td> <td></td> <td>Remove User</td> </tr> <tr> <td>standard</td> <td></td> <td></td> <td></td> </tr> </table>				admin	Username	admin	Change Password	limited	Full Name		Change Name	service			Remove User	standard			
admin	Username	admin	Change Password																
limited	Full Name		Change Name																
service			Remove User																
standard																			

## 2.18.4.1 Local User(s) Account Configuration

There are four built-in “local” accounts, and corresponding built-in groups. The assigned role of each account corresponds to the account name.

- Admin account = Admin Role (Almost ALL service tools access)
- Limited account = Limited Role (No service tool access)
- Service account = Service Role (ALL service tools access)
- Standard account = Standard Role (Few service tools access)

Unless the customer objects, we recommend you to remove the **standard / limited / admin** default users, and use the **service** user to create individual accounts for each actual user in each group.

**NOTE**

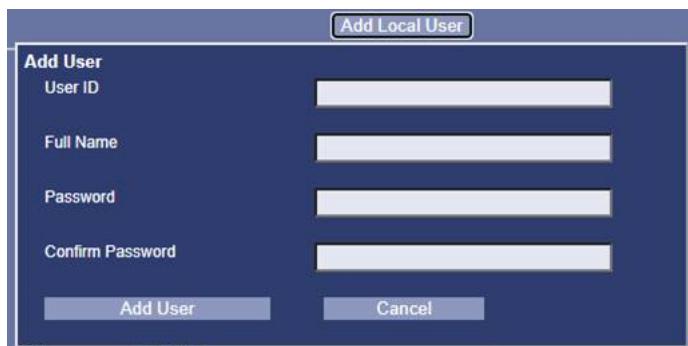
THE “SERVICE” ACCOUNT cannot be removed. It is permanent, and is essential for GEHC service access!

**Create an IT admin user account.**

You will now create a local account for the person who will be responsible for managing site accounts. This is typically the IT admin

- 1.) Select the **Local Users** tab at the top of the page.
- 2.) If possible, have the IT Admin or User Account Administrator observe this procedure to learn how to create and modify users.
- 3.) Click on **Add Local User** at the top right of the page.

The *Add User* window will pop-up.



- 4.) Enter the IT admin's User ID. This will be the “Username” that displays for login and administrative purposes.

**DO NOT CREATE A USER ID NAME WITH SPACES IN IT.**

- 5.) Enter the IT admin's Full Name.
- 6.) Have the IT admin enter the desired password twice (once in “Password” and again in “Confirm Password”). If the IT admin is not there, create a password for them and make a note of it.

**NOTE**

Follow the password rules described in this page to enter the password.”

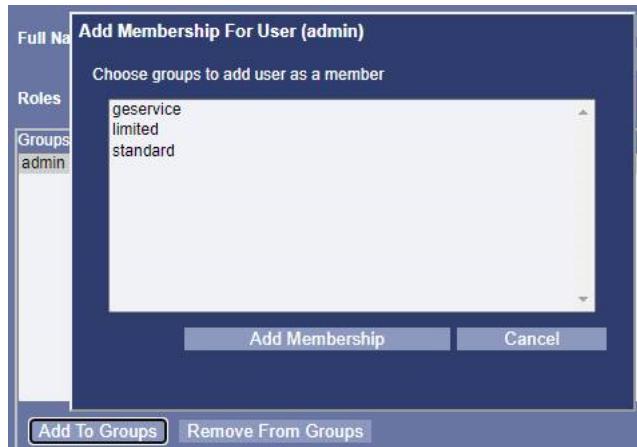
Refer to the guidelines given in [2.21 Job Card IST006 - Changing the Passwords on page 249](#) for choosing a secure password.

- 7.) After completing the user information and password creation, click **Add User**. The new user Username (User ID) and Full Name should now appear in the middle frame area.

**Adding the New User to a Group**

You will now add the new user to one of the existing groups – admin, limited, service, or standard. The group they are assigned to determines their access privileges

- 1.) Click **Add To Groups** at the bottom of the *Group* area of the page.



- 2.) Select the appropriate group for this new user account.
  - If this user account is for the site IT or user admin person, select the admin group.
  - If the user account is for a standard site physician or site user, select the standard group.

User/role access rules are described in detail in the Service Tools Section of the AW Server Service Manual.
- 3.) Click **Add Membership**. The user will be added to the selected group, and the group name will appear in the Groups window.
- 4.) Click on **Apply Configuration** at the bottom of the page.  
The message “Configuration Applied”, with a green background, will be displayed momentarily beneath the “Restore Configuration” buttons if the apply action is successful.  
If it is not successful, there could be a problem with the data entered, or with the system in general.  
Attempt another account creation, and see if it works, or, remove the new account and try the “Apply Configuration” again.
- 5.) If the IT admin wants you to add another user, repeat the above steps of this procedure. Do not add more than two users. Additional users must be added by the customer, NOT by the GEHC FE.  
Once this procedure is demonstrated to the IT or User Account admin, the admin should take over configuring and managing the site's user accounts.

### **“Restore Configuration” button**

The Restore Configuration button restores the last successfully-applied user/group configuration. It does NOT restore “system” configuration.



### **NOTE**

If you have configured a new user, but have not successfully applied it yet, the **Restore Configuration** button will reload the current or last configuration, thus deleting the new user. A new user will not be available for Restore until **Apply Configuration** is successfully applied.

### **Default Passwords**

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

## 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.

### 2.18.4.2 Configuring Enterprise User(s) Accounts

Do this procedure only if the site IT Admin or site User Admin has Enterprise Server information for use. If there is no Enterprise Server data in the Site Survey, and /or IT does not have the data, only Local User Accounts can be configured.

1. Click on **Enterprise** at the top of the page.

The following screen appears.

**Perform Enterprise Authentication, Authorization and Audit configuration**

**Enterprise** (selected)

Enable Enterprise Authentication  
 Cache Enterprise Users

Enterprise Authentication Latency (Seconds): 10

**Configuration Instructions**

Step 0: Attempt to auto-detect the Server Name. Auto-detection will not work on all systems. Manually configuring the Server Name can be done in the next step.

Auto-detect Server Name

Step 1: Enter the Server Name / IP and the authentication type (at right). Click 'Test Connection'

Test Connection

Step 2: Choose the Server Type from the drop-down (at right). Click 'Generate Defaults'

Generate Defaults

Step 3: Make any necessary modifications to the default configuration

Step 4: Attempt to login with your username/password to the Server

Username: [ ] Login  
 Password: [ ]

**Server Configuration**

Server Name / IP: logon.ds.ge.com  
 Authentication Type: Simple LDAP  
 Use SSL  
 Verify Certificate  
 Server Type: Microsoft Active Directory  
 Realm Name: LOGON.DS.GE.COM

**LDAP Configuration**

Format: domain  
 DN: DC=logon,DC=ds,DC=ge,DC=com  
 Login Attribute: sAMAccountName  
 First Name Attribute: givenName  
 Last Name Attribute: sn  
 Group Attribute: memberOf

Apply Configuration | Restore Configuration

2. At the top of the page, enter the following settings:

- **Enable Enterprise Authentication:** This must be enabled (checked) to allow enterprise users to access the server.
- **Cache Enterprise Users:** (The site's IT admin should make this decision.) Checking this box allows users who have previous successful logins to access the server during temporary authentication-server outages.
- **Enterprise Authentication Latency (Seconds):** Set this to 10 seconds unless the IT admin wants a different value. (This determines how long before timeout.)

3. Configure the enterprise server by entering all information needed for the right-hand column (the *Server Configuration* and *LDAP Configuration* areas). There are two ways to do this:

- **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 column. If this method does not complete successfully, use manual configuration.

- Manual Configuration: Enter all configuration data manually, using information from the site survey document and/or the IT admin.

**NOTE**

It is recommended to use an **encrypted communication protocol** (SSL protocol) if available, to avoid passwords to be sent in clear, and a **certificate validation** (check **Verify Certificate** check box just below the **Use SSL** check box) to avoid Enterprise Server to trust any available server certificates. To enable the SSL protocol and use certificate validation, the certificates between the AW Server and the Enterprise Repository shall be exchanged. This will be done later through [2.18.11 Certificate Management on page 211](#).

4. If the site survey document contains only the Active Directory IP, and the authentication with SSL connection fails:

- Ask the IT admin to supply the Active Directory Server certificate Common Name (also called FQDN (Fully Qualified Domain Name)) and use it as **Server Name**.
- Or proceed to the following:
  - a. Open a Terminal tool on the AW Server and login as **root**.
  - b. Type the command:

```
openssl s_client -connect <Active Directory IP>:636 | grep -i  
CONTROLLER
```

The following lines appear:

```
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
```

- c. Copy the Active Directory Server **certificate Common Name** (CN), from the <FQDN> into the **Server Name** field.
  - d. In the *Configuration Instructions* panel, follow instructions from Step 1 to Step 5.
5. Click on **Apply Configuration** (at the bottom of the right-hand column), no matter which configuration method you used.
  6. To verify that the enterprise configuration was successful, do the following steps from the *Configuration Instructions* panel:
    - a. Click on **Test Connection**. If the connection is successful, the message CONNECTION OK (on a green background) appears briefly next to the button.

**NOTE**

If the SSL protocol is used and the certificate verification is enabled, the check will be done later through [2.18.11 Certificate Management on page 211](#).

- b. Enter an enterprise **Username** and **Password**, then click the **Login** button.

For example:



If both tests are successful, the enterprise configuration is correct.

Proceed to [2.18.4.3 Assigning User Roles on page 197](#).

### 2.18.4.3 Assigning User Roles

Assigning roles to new enterprise users determines their access privileges for AW Server applications and/or tools. This is done by mapping the enterprise user account group to one of the existing built-in roles: Administrator, Limited User, GE Service, or Standard User.

1. Acquire group/role information for the enterprise user(s) setup in the site IT Domain. There are at least two ways to do this:
  - Get the information from the site IT Admin or site User Account Admin.
  - Get the information from the **Users (EA3) > Enterprise > Login test utility**. After a successful enterprise login test, the Login Results window will show the information. You may have to scroll down to see the complete information set.

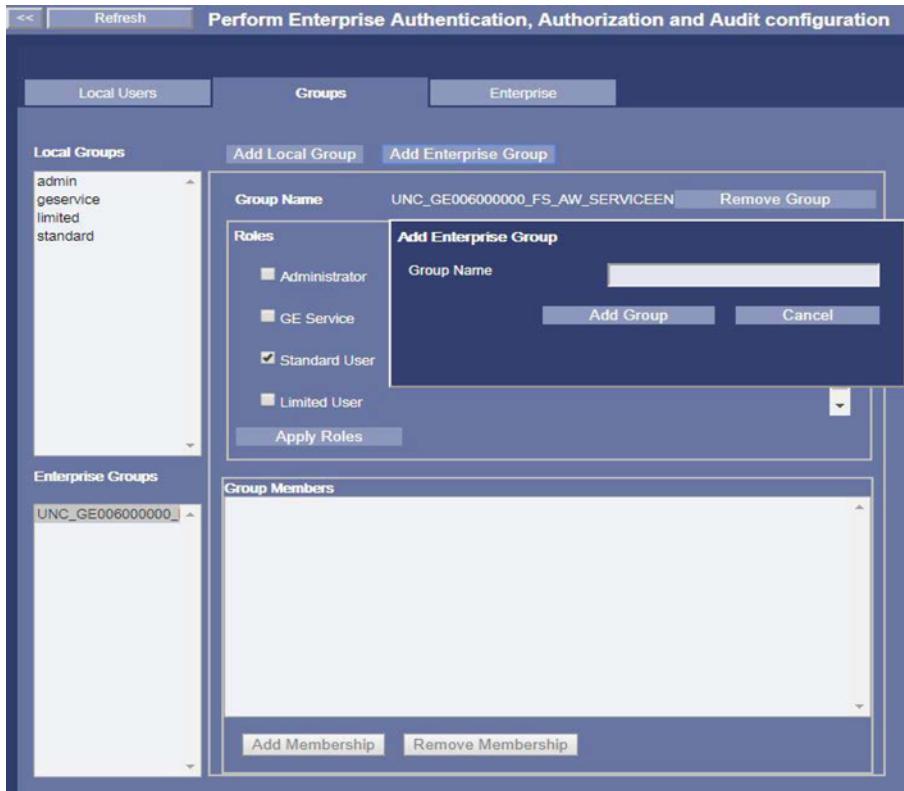
The data of interest in this example is the information starting with “Group Membership”. The data is set up by the administrator of the enterprise server.

#### NOTE

In the *Login Results* window, some browsers might not let you scroll down far enough to see the entire data list if the list extends “below” the bottom of the window. One workaround is to use your left mouse button to select the text and drag the cursor down until the “hidden” information is visible.

2. Click on **Groups > Add Enterprise Group**.

The *Add Enterprise Group* window appears on the top of the *Groups* tab window:



3. Enter the group information acquired from the *Enterprise Login Results* window.
4. Click on **Add Group**.

The added group appears in the *Enterprise Groups* list in the lower left window frame.

5. Click on **Apply Roles**.

A green **Configuration Applied** box briefly appears next to the apply button. If so, the group and role configuration was successful.

Make sure the site IT or account administrator knows how to use these processes to add, delete, and manage their accounts.

## 2.18.5 Users (OS) Password Generation

For the systems connected via RSvP, the system passwords for **root** and **filetransfer** system users/accounts, can be generated and synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault.

These passwords must be changed later in [2.21 Job Card IST006 - Changing the Passwords on page 249](#), [2.21.1.2 Changing Linux passwords on page 251](#).

## 2.18.6 Smart Card configuration

**This feature is only available for sites allowing “two-factor authentication” authentication method and with a specific agreement, as it requires specific integration on site.**

A two-factor authentication method is a two-step verification method using two pieces of evidence (or factor) to authenticate.

AW Server supports client certificate authentication. The client certificate and its private key can originate from the certificate store of the operating system or from tamper-resistant physical devices, such as smart cards or USB tokens, providing two-factor authentication in the latter case.

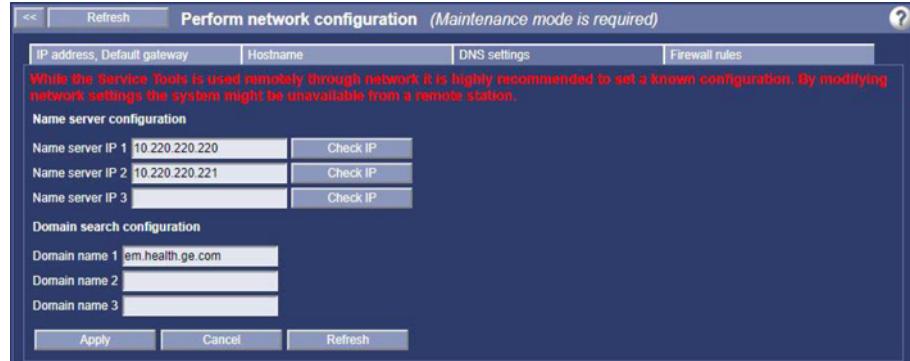
Thus, Smart Card is a two-factor authentication method which improves the security of user login.

**NOTE**

Please contact your GE Sales or Service representatives to check if this feature is available on site.

- 1.) Make sure the AW Server is in Maintenance mode or place it under **Maintenance Mode** on page 571 for details.
- 2.) Make sure that the network configuration is correct:
  - From the Service Tools menu, click on **Maintenance** to expand the menu.
  - Then click on **Network**.
  - Select **DNS settings** tab.

The DNS configuration page displays:



In case the site's DNS server(s) have not been set up during the early installation steps (see [2.13 Job Card IST005 - Network and Time Configuration on page 127](#)), you can configure them through the Service Tool, as described in [A.8.8 DNS server\(s\) setup - Alternate method on page 594](#).

- 3.) Make sure the Time configuration is correct.

Date and time setting and NTP server can be configured from the Service Tools on **Initial configuration** menu and **Time Settings** sub-menu. Refer to Sections [2.15.6.1 Date and Time menu on page 148](#) and [2.15.6.2 Time Server menu on page 149](#).

- 4.) Return to the **Administrative** menu and **Configuration** sub-menu.

Click on **Smart Card Configuration**. The *Smart card login configuration* page displays.

The screenshot shows the 'Smart card login configuration' page. At the top, there is a header bar with 'Smart card login configuration (Maintenance mode is required)'. Below the header, there are several sections: 'Smart Card Login' (with a checked checkbox labeled 'Enable Smart Card Login'), 'Active Directory Configuration' (including 'Server Configuration' with 'Use SSL' checked, and fields for 'Server name / IP' (gaia.sll.se), 'Port', 'Authentication Type' (LDAP using SSL for encryption), 'User' (kmt\_svc\_geaw\_adread@gala.sll.se), 'Password' (redacted), and 'DN' (DC=gala,DC=sll,DC=se)), 'User Mapping' (with fields for 'Login Name Attribute' (sAMAccountName), 'First Name Attribute' (givenName), 'Last Name Attribute' (sn), 'Group Attribute' (memberOf), and 'UPN Attribute' (userPrincipalName)), 'JSON Web Token (JWT) Settings' (with a 'JWT Secret' field containing 713k6h3AZfwyJJSYyNEI50eeWuC3b8sF and a 'Generate' button), and 'Proxy settings' (with 'Direct (No Proxy)' selected, 'Manual Proxy Configuration' disabled, 'HTTP Proxy' set to PTC-Zscaler-EMEA-Amsterdam3PR.proxy.cor, and 'Port' set to 80). A red box highlights the 'Enable Smart Card Login' checkbox, and a red callout box points to it with the text 'Be sure to check here, when Using Smart Card Login'.

- 5.) At the top of the page, enter the following settings:

- **Enable Smart Card Login** – This must be enabled (checked) to allow Smart card authentication.

- 6.) You will now configure the **Active Directory** Settings.

Smart card login uses an Active Directory (LDAP server) to query user attributes and user groups.

To execute queries against the Active Directory server, a dedicated bind user with read privileges is needed.

The service will use the bind user's username (specified in DN or domain format) and password to look up the user's record in the Active Directory.

#### **NOTE**

It is possible to use an LDAP server which is not an Active Directory. In this case the below fields must be properly configured from information supplied by the site's IT Admin.

#### **NOTE**

For the fields below, refer to the site's IT Admin to get the right values and confirm that the pre-populated values are correct.

- **Use SSL** – If secure LDAP is supported, check the **Use SSL** check box. Please refer to the site's IT Admin for more details

#### **NOTE**

If you use LDAP authentication without SSL, user credentials will be sent in clear.

- **Server name / IP** - Enter the name or IP of the Active Directory server (LDAP server).
- **Port** - This is the port on which the LDAP server is listening. Leave empty, except if it is different from 389 for plain LDAP or 636 for secure LDAP.
- **User** - This is the bind user DN, used to bind the actual user and password. It can be specified using an LDAP DN (CN=John Smith,CN=Users,DC=logon,DC=example,DC=com) or using account name and realm name (john@logon.example.com, LOGON\john).
- **Password** - The password for the user name specified in the **User** field.
- **DN** - This is the base DN for LDAP search; it is the point in the LDAP tree from where the service will search for users.

The directory subtree from this node should contain all user records.

If EA3 enterprise authentication is configured, you can use the value as the DN field there.

Specify an LDAP DN such as DC=logon,DC=example,DC=com.

- **Login Name Attribute, First Name Attribute, Last Name Attribute, Group Attribute, UPN Attribute** - These are the Active Directory attributes. They are pre-populated. If not contact your site's IT Admin.

- 7.) **JSON Web Token (JWT) Settings:**

**JWT Secret** - Click the **Generate** button to generate a JSON Web Token secret.

- 8.) **Proxy settings:**

This is used to obtain the revocation of the certificates. By default, **Direct (No Proxy)** is checked.

If the AW Server needs a proxy to address that, check **Manual Proxy Configuration** and enter the following settings (contact the site's IT Admin for the values):

- Set the **HTTP Proxy** (IP or name).
- Set the **Port** (HTTP Proxy port).

**9.) Set up trusted CA certificates:**

This is the bottom part of the *Smart card login configuration* page..

The screenshot shows a configuration interface for managing trusted Certificate Authorities (CAs). At the top, there's a section for "Upload root CA and subordinate CA certificates in PEM format". It includes a file upload input field with the placeholder "Choose Files" and "No file chosen", and a "Send to system" button. Below this is a list titled "Certificates on Server" containing two entries: "siths\_type1\_ca\_v1\_pp.cer" and "siths\_root\_ca\_v1\_pp.cer", each with a small checkbox icon next to it. There are "Remove Selected Certificates" and "Apply configuration" buttons at the bottom.

For a client certificate chain to be considered valid, the issuing certificates must be trusted. Public certificates of root Certificate Authorities and subordinate issuing Certificate Authorities must be uploaded to the AW Server. The files must have a **.cer** extension and be PEM-encoded.

- Download the client CA certificates and upload them to the AW Server using the **Choose Files** and **Send To System** buttons.

The certificates are displayed in the **Certificates on Server** field.

**10.) You can remove a certificate as follows:**

- Select the certificate you want to remove in the **Certificates on Server** field.
- Click on the **Remove Selected Certificates** button.

The certificate is removed from the **Certificates on Server** field.

**11.) Click on **Save Configuration** at the bottom of the page to save the Smart Card login configuration.**

### Assigning Smart Card User Roles

Next, you will assign the new Smart Card user a ROLE, which will determine their access privileges for AW Server applications and/or tools. This is done by mapping the Smart Card user account group to one of the existing built-in roles – Administrator, Limited |User, GE Service, or Standard User.

Acquire GROUP/ROLE information for the Smart Card user(s) setup in the site IT Domain:

- Get the information from the site's IT Admin or site User Account Admin.

**1.) Assigning Smart Card User Roles** is performed using EA3 Enterprise Groups Configuration:

- Click on **Users (EA3)**.
- Click the **Groups** Tab, then click on **Add Enterprise Group**.

The *Add Enterprise Group* window displays.

**2.) Enter the group information acquired from the site's IT Admin:**

- Click on **Add Group**.

The added group should now appear in the Enterprise Groups list in the lower left window frame.

**3.) With the new enterprise group selected, click the appropriate **ROLE** check box in the Roles frame.** Most normal physician or technologist-type users could be assigned to Standard User role (as an example):

- Click on **Apply Roles**.

A GREEN “Configuration Applied” box should briefly display next to the apply button. If so, the group and role configuration was successful.

**4.) Make sure the site IT or account administrator knows how to use these processes to add, delete, and manage their accounts.**

### Setting up Smart Card reader and Windows driver

Smart Card has been tested with

- SITHS cards and the NetID driver supplied by SecMaker
- YubiKey and its Windows driver

Check with your site's IT Admin if ones of the above technology can be used to set up Smart Card reader and Windows driver.

## 2.18.7 Client Timeout

**This feature is not available with the Seamless integration.**

Managing Clients is done through both **Administrative Configuration** and/or **Administrative Utilities**.

Client timeout allows to set up the time limit for inactive client(s) before they are disconnected.

When a client is inactive for the specified period of time, the AW Server will send it a warning message that it is about to be disconnected. If the warning period expires with no acknowledgment from the user, the client will be logged out.

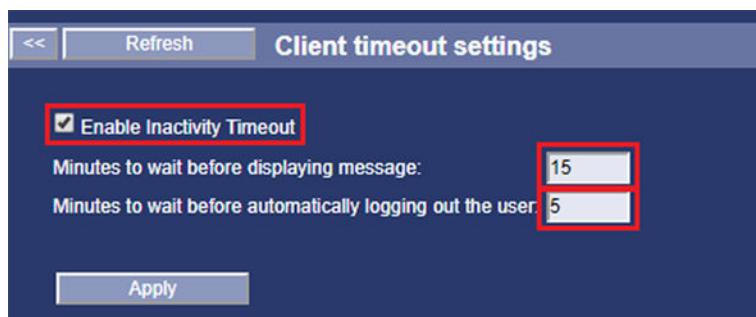
Client timeout is **enabled** by default. However, it can be disabled or updated by the IT administrator of the site.

The warning message (broadcast message) can be set by the IT administrator of the site through [2.18.13 Administrative Utilities on page 221](#).

### Client timeout settings

Use this to set up the time limit for inactive client(s).

1. From the Service Tools menu, click on **Administrative** to expand the menu, then click on **Configuration**, and then select **Client Timeout**.



2. **Enable Inactivity Timeout** is checked to automatically disconnect inactive client(s) after the specified time. Because the AW Server only allows a certain number of slices to be processed, disconnecting inactive client(s) allows other users to have access to the AW Server. If you do not want inactive client(s) to be disconnected, un-check this box.
3. Enter the **Minutes to wait before displaying message** value. The default is 15 minutes. After this amount of time, a default disconnection warning message will be sent to the inactive client(s).
4. Enter the **Minutes to wait before automatically logging out the user** value. The default is 5 minutes. After sending the disconnection message, the Client will wait for this amount of time, and will then automatically auto-disconnect.

#### NOTE

**Note for Integration:** If your site is going to be integrated with RIS or PACS, we recommend to use the following settings for the Client timeout:

- Minutes to wait before displaying message = 20'
  - Minutes to wait before automatically login out the User = 30'
5. When you have configured the timeout settings, click the **Apply** button.

## 2.18.8 Preprocessing Configuration

### NOTE

Entering the pre-processing license is a pre-requisite to configuration.

This shall be done through Initial configuration/Licensing. See section  
[2.15.10.1 Preprocessing configuration menu on page 157](#)

### NOTE

To properly configure Preprocessing, it is necessary that the Volume Viewer applications have been previously installed. See [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#).

This page is used to configure preprocessing. When new instances become available, the AW Server will search the Series Descriptor of the new series for the Series Descriptor words configured in the Service Tool Preprocessing configuration screen.

If a match is found, the corresponding application will start automatically and save the results in a save state series.

For example, if you enter "CTA head" in the descriptor field for Head-AutoBone Xpress, the AutoBone Xpress application will start without user intervention and save the results in a "save state" series.

AW Server becomes aware that new data are available in different ways, depending on the integration mode:

- **No-Integ or Hybrid:** When new data are sent to the AW Server
- **Seamless:** When AW Server receives Notification from PACS (Universal Viewer Server).
- **DICOM Direct Connect:** When AW Server receives a DICOM Instance Availability Notification (IAN) notification from the PACS/VNA.

PACS/VNA must be configured to send IAN notification to AW Server AE-title: **<AWS\_AE-title>\_ds** (do not forget the "\_ds").

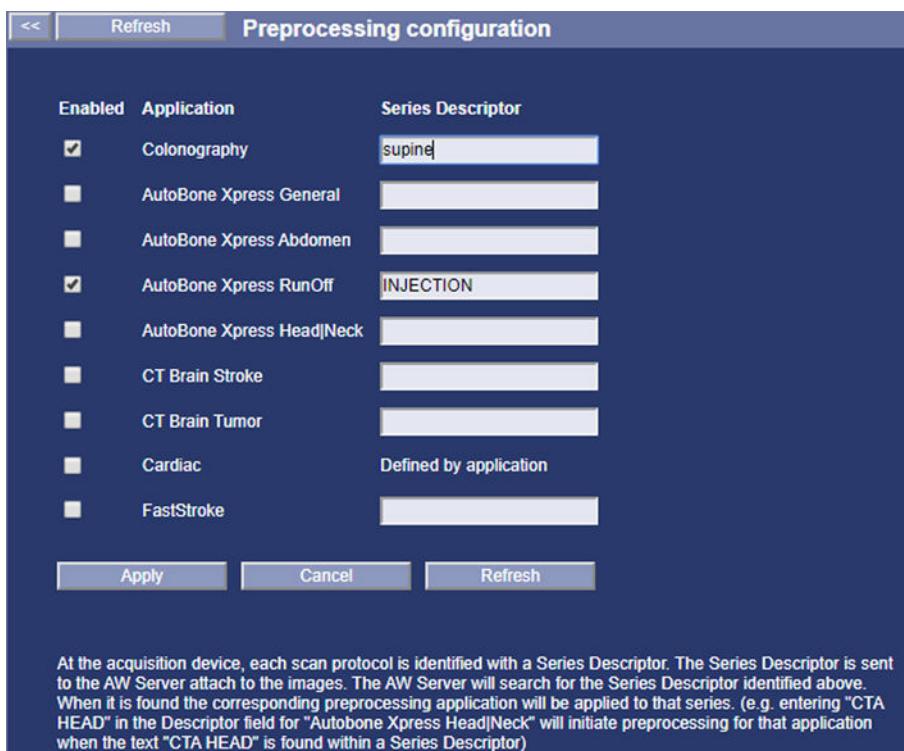
Refer to the EA administrator to configure the IAN notification.

### NOTE

In cluster configuration, the AW Server AE-title of the first node can be used. If this node is in maintenance or shutdown, preprocessing will not work.

1. From the Service Tools menu, click Administrative, then click **Configuration**, then click **Preprocessing**.

What you actually get on the screen may differ from the example below, depending on the Applications installed.



2. Click the box next to an application to make the text box active. See example above.
3. Type in a series descriptor that the AW server will use to search.

If the series description of the new series contains the words entered in the series descriptor box, processing on that series will automatically begin and the results will be saved to a “save state” series.

#### **NOTE**

If the series description of a new series contains words matching multiple configured words, then only the first corresponding application will be launched.

4. After configuring the preprocessing, it is recommended to reboot the AW Server to take into account this functionality. You can also wait and continue with the other configuration steps and reboot later to avoid multiple reboot.
5. After configuring the preprocessing, it is recommended to test the full functionality to ensure configuration is successful:
  - In **No-Integ / Hybrid** integration mode push new series to the AW Server.
  - In **Seamless** integration mode, select a dataset in Universal Viewer browser and click **Verified**.
  - In **DICOM Direct Connect** integration mode, push new series to the PACS/VNA and make sure “IAN” notification is configured on the PACS.

Test that the new "Auto Save State" series created by preprocessing arrives at the destination via the **End of Review** feature.

#### **NOTE**

The **End of Review** shall be configured prior to testing preprocessing.

## 2.18.9 MailSender Settings

You will now configure the MailSender service. This service allows applications, which use email service, to send email reports to predefined contacts/recipients.

**NOTE**

Entering the MailSender license is a pre-requisite to configuration.

This shall be done through **Initial configuration / Licensing**. See section [2.15.10.2 MailSender on page 157](#).

**WARNING**

It remains the responsibility of the user to configure the send by email functionality with a secure mail server and ensure compliance with regulations for email delivery to IT administrative configured recipients.

**WARNING**

The send by email functionality is intended to help facilitate communication between clinicians. Patient management should not be dependent on receipt of email communication.

**WARNING**

Email content contains limited PHI such as a unique exam identifier and time of scan.

1. Display the MailSender Settings page:

From the **Service Tools / Administrative** menu, click on **Configuration** then on **MailSender**.  
The MailSender service page displays:

The screenshot shows the 'MailSender Configuration' page. Key fields highlighted with red boxes include:

- Enable MailSender?**: Radio button selected for "Yes".
- Sender Address\***: Input field containing "no-reply.appname.aws-hostname@hostpital.com".
- SMTP Server Address\***: Input field containing "192.168.10.32".
- SMTP Server Port\***: Input field containing "587".
- SMTP Security Level\***: Drop-down menu set to "TLS".
- SMTP Server CA Certificate**: "Choose File" button pointing to "ca.crt" and an "Upload" button.
- Expiration date:**: Text field showing "Mon Sep 29 10:29:02 CEST 2025".
- Notification Address\***: Input field containing "notif.address@hospital.com".
- Test Mail Sending**: "Test Connection" button.
- Disclaimers** section:
  - Warning: It remains the responsibility of the user to configure the send by email functionality with a secure mail server and ensure compliance with regulations for email delivery to IT administrative configured recipients.
  - Warning: The send by email functionality is intended to help facilitate communication between clinicians. Patient management should not be dependent on receipt of email communication.
  - Warning: Email content contains limited PHI such as a unique exam identifier and time of scan.
- Buttons at the bottom:** "Apply" (highlighted with a red box) and "Cancel".

2. Enable the MailSender service:
  - Check the **Enable MailSender** chek box.
3. Configure the local SMTP mail server:
  - Enter the mail sender address in the **Sender Address** field.

#### NOTE

You only need to enter the domain name of the hospital's mail address, the part after @.

#### NOTE

This is the email address of the sender of the email. It will contain the name of the application and the name of the host corresponding to the application/host from which the report will be sent. The user will not be able to reply to this address.

- Enter the mail server address (enter IP address or fully qualified domain name) in the **SMTP Server Address** field.

#### NOTE

Refer to the site's IT Admin to obtain the local mail server address.

- Enter the mail server port number in the **SMTP Server Port** field.

**NOTE**

Refer to the site's IT Admin to obtain the actual port number.

- Select the mail server security level (**TLS** protocol with usually port **587** or **No** for plain SMTP with usually port **25**) in **SMTP Security Level** field.

**WARNING**



For security reasons, use of plain SMTP mail sending is highly discouraged. Using a **TLS** service is strongly advised for security purposes.

**NOTE**

If using a TLS service, to reinforce security level, the AW Server enforces TLS1.2 for all TLS connections. In case the SMTP server does not support TLSv1.2 protocol, the MailSender will not be able to communicate with it through TLS. In this case and in case the SMTP server supports only plain text communication, then set the **SMTP security level** to **No** in MailSender configuration page.

4. Upload the SMTP Server CA Certificates:

- Click on **Choose File** and select the root CA certificate of the Hospital's SMTP server in the window that opens.

**NOTE**

Refer to the site's IT Admin to obtain the root CA certificate.

- Click on **Upload** to upload the CA certificate to the AW server.

**NOTE**

You can remove the CA certificate by clicking on the **Remove** button.

- In case there are multiple CA certificates in the signing chain of the Hospital's SMTP server's certificate, then import all of them (except the root CA certificate) to the AW Server:

- Gather all the certificate files of all the CA certificates from the signing chain listed in the Certification Path of the Hospital's SMTP certificate. Consult the local IT Admin on how to get the certificate files of the certificates from the signing chain.
- Upload all the signer certificate files to the AW Server. From the Service Tools, select **Tools > File Transfer**, then select **To System** tab.

The files will be uploaded to the /var/lib/ServiceTools/upload directory.

- Open a terminal, login as **root**.

- For all the uploaded certificates execute the following command:

```
keytool -importcert -keystore /etc/mailsender-service/cacerts
-file <URL of the crt file> -alias <unique alias name> -storepass
changeit <Enter>
```

Where **<unique alias name>** should be a unique text identifier (alias name) for the given certificate.

**NOTE**

Alias name "mailsender\_selfsigned\_certificate" is already occupied. Do not use it.

For example if the file name of the uploaded certificate was **smtp\_ca1.crt** then the command will look like this:

```
keytool -importcert -keystore /etc/mailsender-service/cacerts
-file /var/lib/ServiceTools/upload/smtp_ca1.crt -alias smtp_ca1
-storepass changeit <Enter>
```

- e. The command will write details of the execution to the terminal and finally following question appears:

Trust this certificate? [no]:

Type: yes <Enter>

The following message appears: Certificate was added to keystore

That means that the command was executed successfully.

- f. Execute the following command:

```
systemctl restart mailsender-service.service <Enter>
```

- Enter the **Notification Address** email to notify the customer on certificate expiration.

#### NOTE

This is **not** the address on which emails generated by applications will be sent to. Refer to the site's IT Admin to obtain the email address.

The following messages will display in the Service Tools when the root CA certificate expire soon or has expired

**Active Service Tools tasks: 0**

- Global Installed Base data is not sent yet to GE!
- The SMTP TLS certificate for email sending has expired. [Click here for details.](#)

**Active Service Tools tasks: 0**

- Global Installed Base data is not sent yet to GE!
- The SMTP TLS certificate for email sending will expire soon. [Click here for details.](#)

Click on **Click here for details** to open the MailSender configuration page.

5. Test the connection:

Click on **Test Connection** button to check that the SMTP server accepts SMTP connection with the selected security level.

The **Success** label highlighted in green displays momentarily if the connection is successful.

6. Click on **Apply** button to save the information entered.

### 2.18.9.1 Configure the contact/recipient

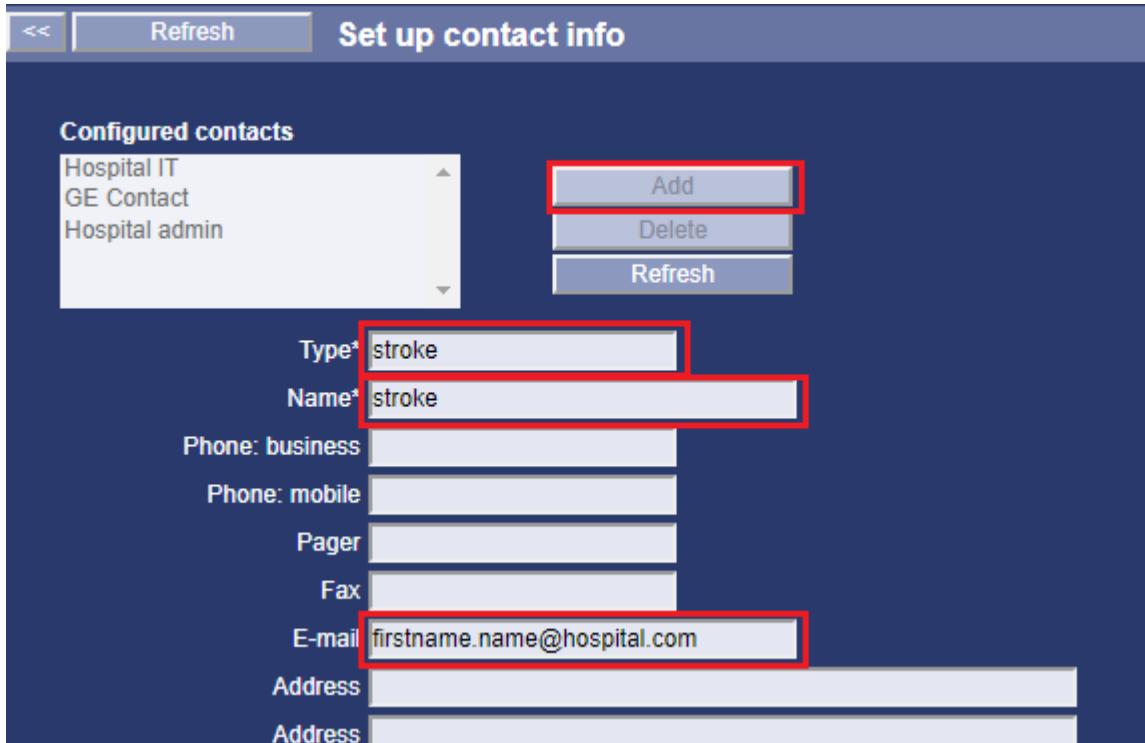
Each application using the email service shall configure the email address of the recipient(s) to which it will send the reports.

#### NOTE

Perform this steps when installing the applications which uses the email service. **This is described in the corresponding application service documentation.** Below is an example for FastStroke application.

1. From the **Service Tools / Initial Configuration** menu, click on **Contact** to display the Set up contact info page.

2. Select **Add** button to configure an email application contact.



3. In the fields that displays, enter the **Type**, the **Name** and the **E-mail** address of the recipient.

**NOTE**

**E-mail** is the address to which generated email will be sent.

**NOTE**

You can enter several email addresses separated by a comma.

**NOTE**

Refer to the site's IT Admin to get the email address(es).

**NOTE**

Check the spelling and the format of the email address(es) you enter. A mistype address may lead to a **failure** of the MailSender functionality as the recipients may not receive the letters.

4. Click on **Apply** button to save the information entered.

## 2.18.10 End of Review

This tab is used to configure "End of Review" processes. When enabled, the End Of Review feature automatically sends processed images to a DICOM host when exiting the application (at tab closure). It is configurable to send which image: "all" or "generated".

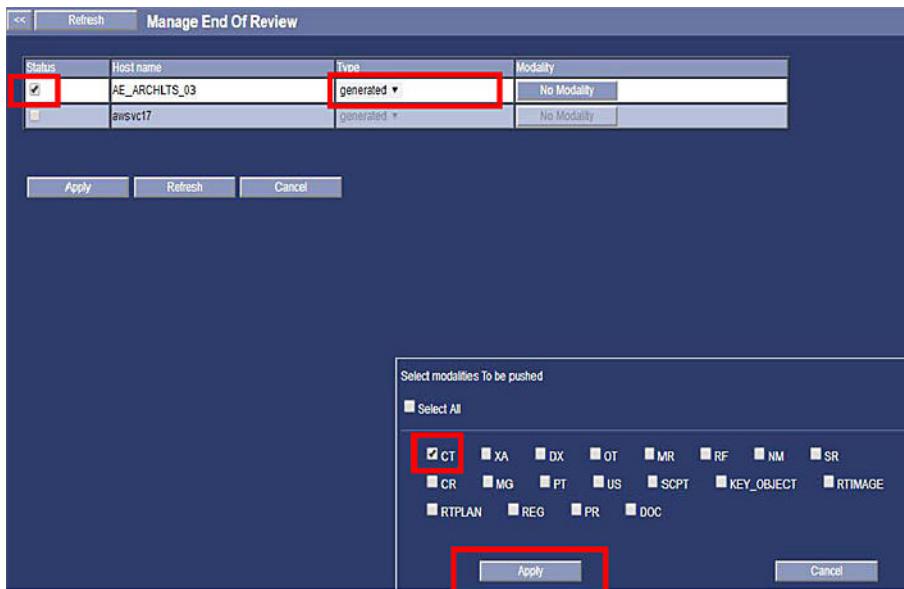
After completing a processing procedure, when the Users exit from the feature, they are prompted to choose whether you want to end review. If you choose yes, the AW Server automatically forwards the processed series to any DICOM host connected to the server.

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.

**NOTICE**

The Seamless Integration must be fully configured prior to configure End Of Review.

- From the Service Tools menu, select **Administrative > Configuration > End of Review**.



- In the *Manage End Of Review* page, under the **Status** heading, click the box next to the host name to enable the “End of Review” process.
- Use the drop-down menu under **Type** to select which series (**generated**, or **all**) will be automatically sent to a networked host upon exiting an application.
- Click the button under **Modality** to view all modality choices.
- Click **Select All** or any combination of individual modalities that you want to be automatically sent and click **Apply**.
- Click **Apply** to save the changes.

**NOTE**

When the End Of Review configuration is changed, the change does not become instantly effective for users that are logged-in, but will become effective starting from the next login session.

## 2.18.11 Certificate Management

This section describes the management of the certificates files on the AW Server. It describes how to:

- Import a certificate file to the AW Server trust store.
- Associate a certificate with a feature (copy the certificate to a specific trust store).
- Export the AW Server certificate file to an external system.
- Renew an expired external certificate.
- Renew the AW Server certificate.

**NOTE**

This procedure can be used to upload, import and/or renew any external certificate file needed by the AW Server and renew the AW Server certificate.

It also allows to associate an external certificate with a feature (copy the certificate to a specific trust store). Right now it is limited to support secure connection to a DICOM host, connection to a log server to send Audit log (EAT) messages securely, EA3 secure connection to the Customer's Enterprise Authentication server and for secure integrations with other GE systems.

## 2.18.11.1 Importing a certificate file to the AW Server trust store

The AW Server certificate file format requirement is the following:

- AW Server supports the X.509 Linux based encoding scheme (extensions .pem, .crt, .cer).
- Does not support the DER encoding scheme.

The Certificate Management tool allows to import a certificate present on the FE's laptop or on USB media or uploaded into the AW Server.

1. Copy the certificate file into a GE validated read/writeable USB media.

**NOTE**

For non-GE systems, ask the local IT admin to copy the certificate file to a GE validated read/writeable USB media.

2. Insert the USB media into the FE's laptop.
3. From the Service Tools, select **Administrative > Configuration > Certificate Management**.

The Certificate Management page displays:

#	Certificate	Expiry Date	Applications / Namespaces	Actions
Total certificates on device 0				

**Import Certificate : Get the certificate into this machine from a USB or type the certificate URL**

**Import Third Party Certificate**

**Configure Certificate : Map the certificate to components**

**Configure Certificate**

**Certificate Name**  
awsvc244Certificate

**Certificate URL**

(OR)

**Import from local computer**  
awsvc244.crt

**Browse**

**Submit** **Reset**

4. In the **Trusted Certificates** tab, click on **Import Third Party Certificate**.
5. Enter a name for the certificate into the **Certificate Name** field.

**NOTE**

It is important to use a relevant certificate name as several certificate files from different systems can be imported.

6. Click on **Browse** and select the certificate file stored on the USB media.

The certificate file name is displayed in the **Import from local computer** field.

7. Click on **Submit** button.

8. The certificate file is saved and added to the AW Server trust store. It is displayed in the certificates table.

#	Certificate	Expiry Date	Applications / Namespaces	Actions
1	awsvc244certificate	25/06/2026		
Total certificates on device 1				

#### NOTE

The certificate can be viewed, deleted or downloaded using one of the 3 icons in the **Actions** column of the table.

#### NOTE

The Certificate Management tool allows also to import a certificate uploaded into the AW Server.

To upload a file into the AW Server, in the Service Tools select **Tools > File Transfer**, then select **To System** tab. The file will be uploaded to the `/var/lib/ServiceTools/upload` location.

Then follow steps [Step 3](#), [Step 4](#) and [Step 5](#), enter the certificate file (full path) into the **Certificate URL** field, and follow steps [Step 7](#) and [Step 8](#).

## 2.18.11.2 Associating a certificate with feature(s)

Associating a certificate with a feature allows to copy the certificate to the corresponding trust store.

1. From the **Trusted Certificates** tab, click on **Configure Certificate** button.

#	Certificate	Expiry Date	Applications / Namespaces	Actions
1	awsvc244certificate	25/06/2026		
Total certificates on device 1				

**Import Certificate :** Get the certificate into this machine from a USB or type the certificate URL

**Configure Certificate :** Map the certificate to components

**Certificates**

awsvc244certificate

**Namespaces**

**Applications**

audit log  
 enterprise authentication  
 integration  
 dicom

2. Select a certificate name, previously imported, under **Certificates**.

3. If applicable, check the associated feature(s), below **Applications**:

- **audit log** for an Enterprise Repository server.

#### NOTE

If the Imaging Cockpit components have been installed, in the **Namespaces** pulldown menu select **edison-core**.



- **enterprise authentication** for an Enterprise user accounts (LDAP or Kerberos protocol).
- **integration** for AW Server integrated within the CT Console (NanoCloud).
- **dicom** for DICOM trust store.

**NOTE**

If the Imaging Cockpit components have been installed, in the **Namespaces** pulldown menu select **cockpit**.



4. Click on **Submit** button.

The associated feature(s) display in the certificates table under the *Applications / Namespaces* column. The certificate is added to the corresponding trust store (in the example below, the certificate has been associated with the **dicom** feature).

#	Certificate	Expiry Date	Applications / Namespaces	Actions
1	awsvc244certificate	25/06/2026	dicom	

Total certificates on device 1

5. If the certificate was associated with the **dicom** feature or you have selected **edison-core** Namespace for **audit log**, then reboot the server. From the Service Tools, select **Tools > Reboot**.

### 2.18.11.3 Exporting the AW Server certificate file to an external system

1. From the Certificate Management page, select the **AW Server Certificate Info** tab.

AW Server Certificate	
Subject	C=USST=MassachusettsL=BostonO=General Electric Companydevops.aw.health.ge.com
Issuer	C=USST=DEL=WilmingtonO=Corporation Service CompanyTrusted Secure Certificate Authority 5
Expiration Date	Sun 19 Jun 2022 01:59:59 AM CEST

EC Certificates	
Expiration Date	Thu 21 Jul 2022 06:08:00 PM CEST

**Download certificates**

2. Click on **Download certificate**.

3. The certificates are downloaded in a zip file. Locate it and unzip it.
  - a. If the AW Server has a self-signed certificate, then the zip file contains the `ca.crt` (Certificate Authority certificate) and the `server.crt` (AW Server certificate) files.
  - b. If the AW Server was signed with an external CA certificate, then the zip file will contain only the `server.crt` (AW Server certificate) file.

**NOTE**

Double-click on the `server.crt` file and then click on **Open** in the pop-up dialog to run the file. The upcoming dialog will display the information about the Certificate Authority certificates in the **Certification Path** tab. Consult the local IT Admin on how to get the CA certificates listed in the **Certificate Path**.

4. Copy the certificate files to a GE validated read/writeable USB media.
5. On the external system, insert the USB media and copy the certificate files in the local trust store.

**NOTE**

Depending on the external system type, the procedure may differ. For non-GE remote system refer to the local IT admin, otherwise refer to the related documentation.

**NOTE**

This page contains, in the first part, the AW Server certificate expiration date, and in the second part, the AW Server Web Client certificate expiration date (if it has been installed and activated).

## 2.18.11.4 Renewing an expired external certificate

If a certificate has expired, delete it and reimport it to the AW Server:

1. From the Service Tools, select **Administrative > Configuration > Certificate Management**, then select the **Trusted Certificates** tab.
2. Dissociate the certificate from the associated feature(s).

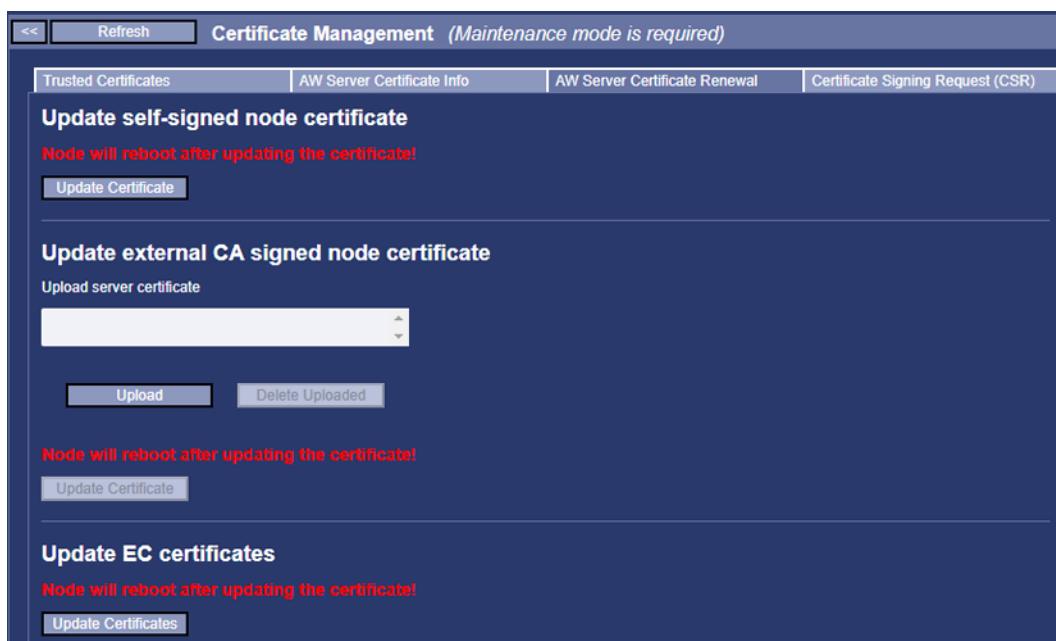
If the certificate is associated with feature(s), they display in the certificates table under the *Applications / Namespaces* column.

In this case follow the below steps to dissociate the certificate from the feature(s):

- a. Click on **Configure Certificate** button.
  - b. Below **Certificates**, select the certificate name that will be deleted and uncheck the associated feature(s), below **Applications**:
    - **dicom** for any DICOM Host.
  - c. Click on **Submit** button.
3. In the certificates table, locate the certificate name and select .
  4. In the popup window, click on **Confirm** button.
  5. Reimport the certificate file as described in [2.18.11.1 Importing a certificate file to the AW Server trust store on page 212](#).
  6. Reassociate the certificate with feature(s) as described in [2.18.11.2 Associating a certificate with feature\(s\) on page 213](#).

## 2.18.11.5 Renewing the AW Server certificate

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

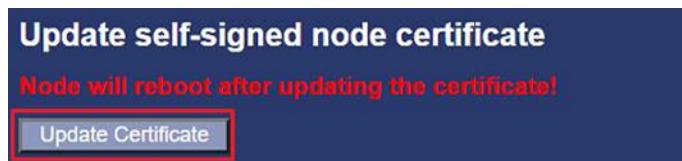


#### NOTE

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

#### 2.18.11.5.1 Renewing AW Server self-signed certificate

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



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



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



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



## 2.18.11.5.2 Renewing AW Server external CA signed certificate

This section allows to generate an AW Server certificate signed by an external certificate authority, by:

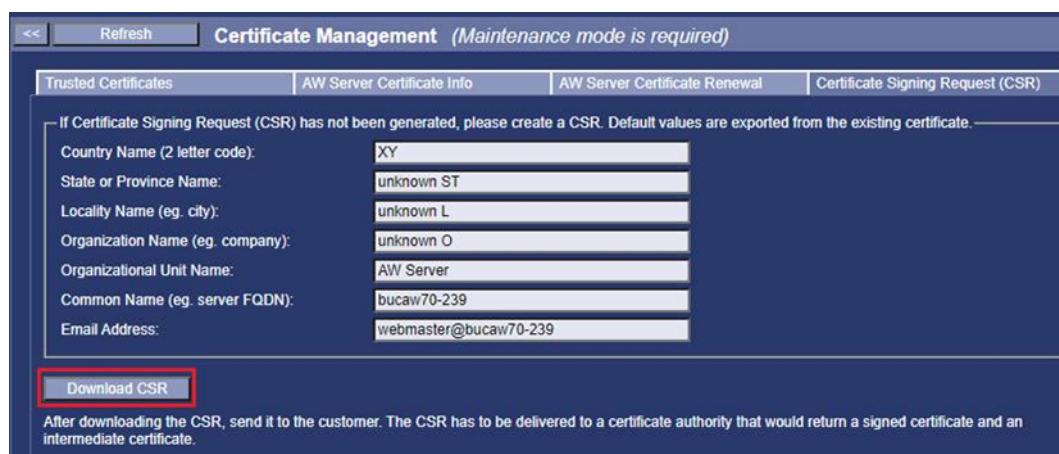
- Generating a Certificate Signing Request (CSR).
- Exporting the AW Server certificate as CSR to be signed by external authority.
- Importing the trusted certificate to the AW Server.

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.

1. Generating a Certificate Signing Request (CSR):

- a. Select the **Certificate Signing Request (CSR)** tab.

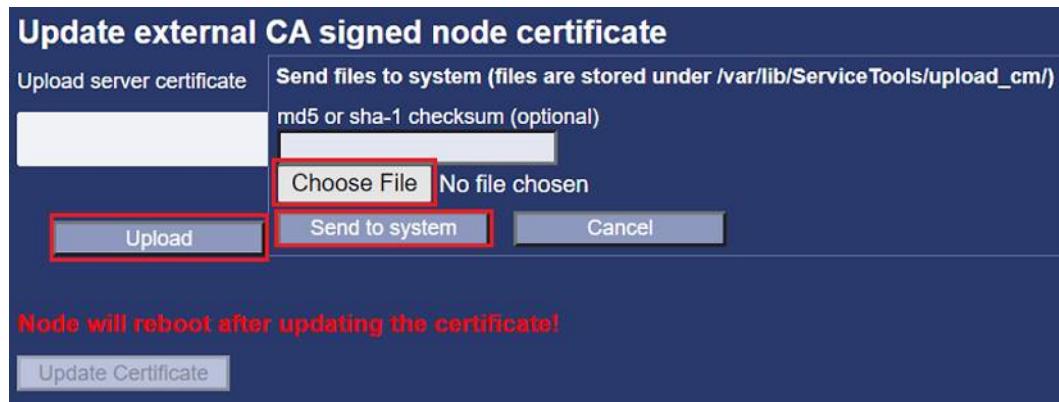


### NOTE

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. Return to 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.

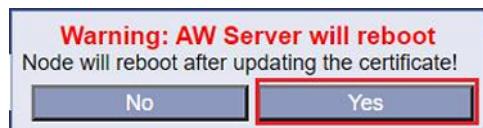
**NOTE**

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.



### 2.18.11.5.3 Renewing AW Server Web Client certificate

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

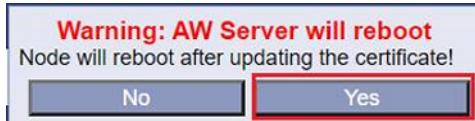
1. In the *Update EC certificates* part of the page, click on **Update Certificates**.



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



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



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



## 2.18.12 AW Server declaration on DICOM images sources

The following is given for information only.

To declare your AW Server system to all the DICOM hosts (Image sources (i.e: CT, MR, etc.) which will send images to the AW server proceed as follows. Note that the AWS HealthPage displays the host name and AET.

- Host name: Enter AW Server host name
- **Application Entity Title (AET)** = Must be same as the host name

If the Host name of the AW Server is longer than 16 characters, the first 16 characters of the Host name will be used as AE Title for the AW Server

- **Port number** = 4006 for AW Server
- Query/Retrieve = supported

### NOTE

Bypass this step for Full or Seamless integration. This step is not necessary, as a fully integrated AW Server does not host an image database. The image data is only resident on the PACS.

### 2.18.12.1 DICOM Direct Connect integration

For DICOM Direct Connect integration, the AW Server shall be declared twice in the DICOM hosts (PACS, VNA, etc.) which will send images to the AW server:

- One entry with the AW Server <host name>/<AET>, IP and port **4006** (as described in [2.18.12 AW Server declaration on DICOM images sources on page 219](#) above) for standard DICOM functions.

**NOTE**

For secure connection (DICOM TLS), use the secure port **2762**.

- The second entry with the AW Server <host name>**\_ds**/<AET>**\_ds**, same IP and port **4010** for DICOM Direct Connect.

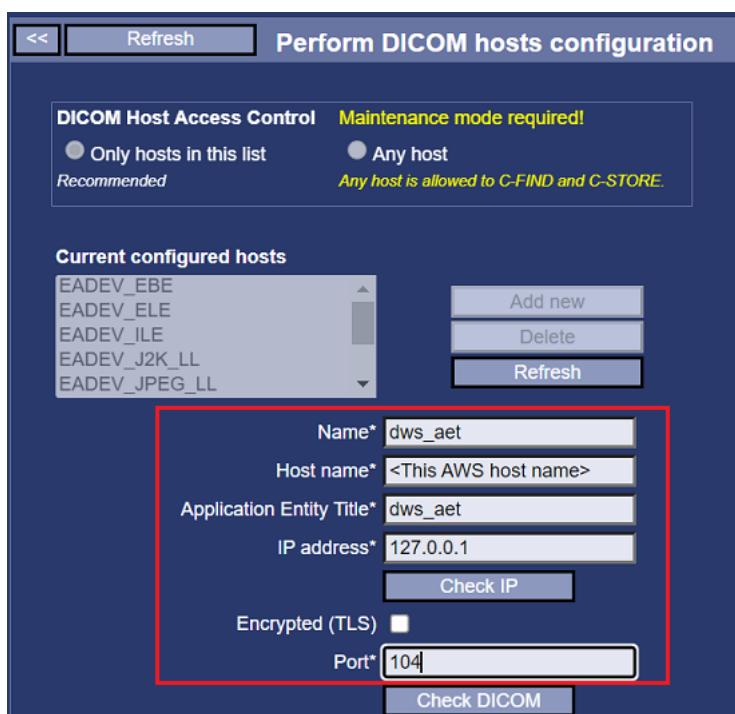
**NOTE**

For secure connection (DICOM TLS), use the secure port **4020**.

## 2.18.12.2 Imaging Cockpit / AW Server Web Client

To ensure DICOM communication between the Web Client and a DICOM hosts (PACS, VNA, etc.), follow the below steps:

1. Declare a dummy DICOM host on the AW Server:
  - a. From the Service Tools, select **Administrative > Configuration > DICOM Hosts**.
  - b. Click on **Add new** button and fill in the required fields highlighted in the screen capture below:



In the **Host name** field, replace <This AWS host name> by the AW Server **Hostname** displayed in the Healthpage.

- c. Click on **Apply** button.
2. The AW Server shall be declared 3 times in the DICOM hosts (PACS, VNA, etc.) which will send images to the AW server:
  - One entry with the AW Server <host name>/<AET>, IP and port **4006** (as described in [2.18.12 AW Server declaration on DICOM images sources on page 219](#) above) for standard DICOM functions.

**NOTE**

For secure connection (DICOM TLS), use the secure port **2762**.

- The second entry with the AW Server <host name>\_ds/<AET>\_ds, same IP and port **4010** for DICOM Direct Connect.

**NOTE**

For secure connection (DICOM TLS), use the secure port **4020**.

- The third entry with dws\_aet as host name/AET, same IP and port **104** for DICOM Web services.

**NOTE**

For secure connection (DICOM TLS), use the same port number.

## 2.18.13 Administrative Utilities

**NOTE**

*Administrative Utilities* menu does not contain tools or steps necessary at installation time.

*Administrative Utilities* are described in the Advanced Service Manual, as well as in the Administrator's documentation.

The Administrative configuration is complete

**Proceed to** [2.19 Job Card IST011 - Integration on page 221](#).

## 2.19 Job Card IST011 - Integration

### 2.19.1 Foreword

#### 2.19.1.1 Integration modes supported with AW Server

There are currently **6** different modes of PACS/RIS/DICOM Remote Host integration that can be met on AW Server.

**1. Standalone (No integration):**

In this "non-integrated" mode, the AWS system will be totally independent from the PACS.

GEHC HCS will ensure sales, configuration and service of AW Server.

**2. Full front end integration (Hybrid):** (3rdPartyIntegration)

- 3rd Party integration and Hybrid integration share the same license key and setup menu.
- 3rd Party integration will only be accessible for upgraded AW Server 2.0 that were using this mode.

In this integration mode, the AWS system hosts its own database. Selection synchronization will be maintained between the remote host and AWS. No other synchronization will be available.

In Hybrid mode, the integrated AW Server client pulls the images DIRECTLY from the AW Server database and REQUIRES them to ALREADY be present in the AW Server database PRIOR to launching the integrated AWS client from the PACS client, otherwise the AWS client launch will fail.

There is no automatic Query/Retrieve of the images from PACS in Hybrid mode. Images must be pushed from the modality or from PACS ahead of launching the integrated AWS client. Most likely the site will configure the CT and MR scanners to automatically push each series to the AW Server.

- The target remote systems are the RIS, the competitor PACS (3rd Party PACS) and any other systems (like CT acquisition console for instance).
- GEHC HCS will ensure sales, configuration and service of AW Server.
- See [2.19.2 Full front end integration \(Hybrid\): \(3rdPartyIntegration\) on page 224](#)

### 3. Seamless integration with the GE PACS

In seamless integration mode the image database is on the PACS only. There is nevertheless an internal database for AW Server, intended to store the data generated on AW Server, before the data is automatically sent to the GE PACS.

In addition, the Seamless integration will add a "3D Apps" button to the GE PACS Client Universal Viewer, and when selecting an exam and clicking on the 3D Apps button, this will propose a choice of currently supported 3D applications (purchased by the customer) and launch the AW Server Client window.

Moreover, the viewer events and actions of the GE PACS system in Universal Viewer are synchronized with the AWS application (e.g. mouse modes, paging, lights on/off).

- The targeted remote system is the GE PACS
- EDS will ensure sales, configuration and service of AW Server.
- See [2.19.3 Seamless Integration on page 228](#)

Scalability:

- Multiple AW Server nodes can be configured in a cluster (scalable solution).

### 4. DICOM Direct Connect integration

In the DICOM Direct Connect integration mode, the image database is on the configured DICOM storage providers (PACS/VNA/DICOM Remote Host) only. Nevertheless, the AW Server has also a local database (which is not visible to the user) to store generated data. Using the End Of Review feature, generated data can be sent to the PACS/VNA/DICOM Remote Host.

Two user workflows are supported:

- a. Without 3rd party front-end integration – using the AW Server client

In this mode, the user selects the remote data in the AW Server client using the remote host worklist, then launches the application.

- b. With 3rd party front-end integration – using an integrated PACS/VNA client

In this mode, the user selects the data in the PACS/VNA's client and launches the application. The PACS/VNA client passes the selection to the AW Server, and the AW Server retrieves and loads the data from the remote system. (Here we need a reference for front-end integration configuration).

Configuration:

- The PACS/VNA/DICOM Remote Host(s) must be declared on the AW Server as a DICOM host.
- The End Of Review feature must be configured to send generated data to the PACS/VNA/DICOM Remote Host.
- AW Server must be declared on the PACS/VNA/DICOM Remote Host twice:
  - AE\_title\_AWS, port 4006
  - AE\_title\_AWS\_ds, port 4010

Scalability:

- Multiple AW Server nodes can be configured in a cluster (scalable solution).

See [2.19.4 DICOM Direct Connect integration on page 238](#) for full integration details.

#### **NOTE**

VNA stands for “Vendor Neutral Archive”. It is a DICOM images archiving system.

### **5. DICOM Direct Connect in CT/MR Smart Subscription on Edison HealthLink environment**

The AW Server in DICOM Direct Connect integration mode can run on the Edison HealthLink of the CT/MR Console environment and retrieves the data from the CT/MR Console database.

The AW Server client is integrated within the CT Console Client or on customer desktop for MR Console.

- Refer to [2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink on page 307](#) for full description
- See [2.19.4 DICOM Direct Connect integration on page 238](#)

### **6. DICOM Direct Connect in CT Console environment**

The AW Server in DICOM Direct Connect integration mode can run in a Virtual Machine hosted by the CT Console and retrieves the data from the CT Console database. It is called the NanoCloud AW Server.

- Refer to CT documentation for full description.
- See [2.19.4 DICOM Direct Connect integration on page 238](#)

## **2.19.1.2 Pre-requisite for Integration**

### **Database**

- **Full front end integration (Hybrid):** (3rdPartyIntegration) mode: All patient and Study data must reside on the AW Server and the 3rd party PACS prior to performing integration. The DICOM patient and study data can be sent from the PACS system to the AW Server, or the user needs to query and retrieve the data. Since in Full front end integration it is a prerequisite to have all exam data available on AWS at application launch time, AWS database could be pre-populated from the PACS. AW Server may query and retrieve the data.
- **Front end & backend integration** (Seamless and DICOM Direct Connect mode): Image data are in the PACS database. They do not need to be in the AW Server database, which only contains reconstruction images prior to send them to the PACS database.
- Modality devices shall be configured to send images (auto-push) to both the AW Server and the PACS to ensure the databases contain the same information. Note that this is not necessary in the Seamless integration (using the PACS database).

### **Software license key**

- A software license key is required to enable Integration between the AW Server and a RIS, 3rd Party PACS or GE PACS. License key is different for the different types of integration.

### **DICOM configuration**

- The RIS or PACS system shall be properly declared as a DICOM Host in AW Server
- When configuring DICOM information for PACS Query Retrieve - Allow Query, Allow Retrieve, Allow Store shall be enabled.
- PACS systems supporting Storage Commitment shall be configured on the AW Server.

### **End Of Review**

- End of Review configuration is mandatory for Full front end integration and Front end & backend integration. It is optional, but recommended for Basic front end integration..
- The TYPE of images to be sent to the PACS system when configured shall be set to "generated".

- All modality image types shall be enabled, unless the receiving PACS system does not support a particular image type, then do not select this type of image.

### Pre-processing

- Pre-processing is not mandatory to be configured when integrating to PACS, but would improve the perceived performance.
- AW Server requires a software license key to enable the Pre-processing feature.

### AW Server Client

- AW Server Client must be downloaded and installed on the RIS/PACS workstations where integration will be used by the customer.
- The directory path and executable (if not configured differently) are located on a client in:  
C:\Program Files (x86)\GE\AWS\_3.2\solo\integration.exe

### PACS Connector Plugin

- This is a piece of software delivered with the GE PACS, that shall be loaded on the AW Server for full front end & back end integration with the GE PACS. Currently, for the Enterprise Archive (EA) PACS, it is delivered on a CD media. Refer to the GE PACS documentation for installation instructions.

### PACS Integration Guide

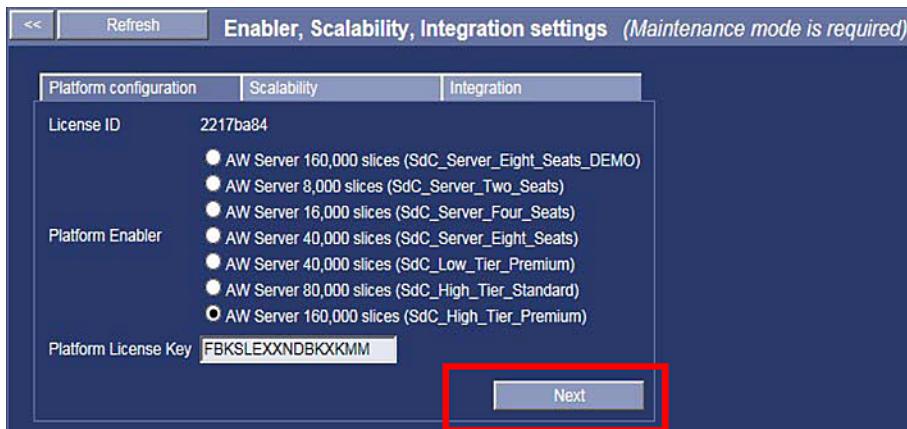
- As part of an AW Server and RIS/PACS integration, provide the AW Server 3.2 PACS Integration Guide document - **5535310-1EN** to the RIS/PACS person so that they may configure the RIS/PACS for the AW Server.

## 2.19.2 Full front end integration (Hybrid): (3rdPartyIntegration)

### 2.19.2.1 Configuration steps on the AW Server

1. Make sure the AW Server is still in Maintenance mode or place it under **Maintenance**. Refer to [A.4 Maintenance Mode on page 571](#) for details.
2. From the Service Tools menu, click on **Initial Configuration** to expand the menu.
3. Click on **Platform Configuration**.

The following menu displays:



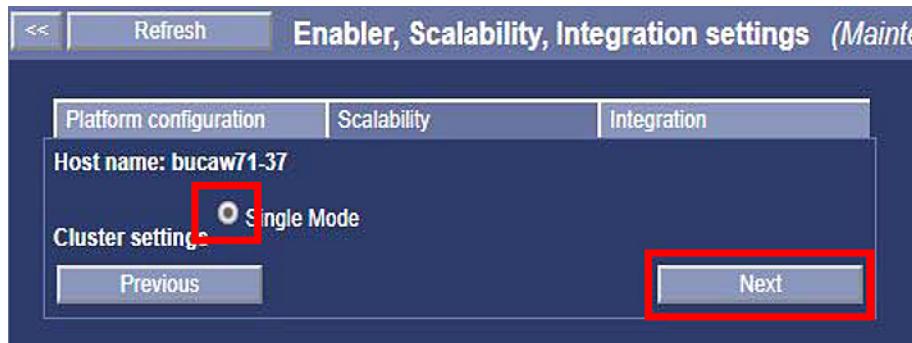
Refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#), section [2.15.9 Platform Configuration on page 153](#) for details.

4. Make sure the “Platform Enabler” license has been entered. If not, enter it now.

5. When done, click on the **Next** button to change to the *Scalability* tab.

#### 6. **Scalability: Virtual AW Server to be placed into a cluster of virtual AW servers:**

Scalability is only supported for Seamless and DICOM Direct Connect integration and with virtual AW Server.



Keep Single mode selected and click on the **Next** button to change to the *Integration* tab

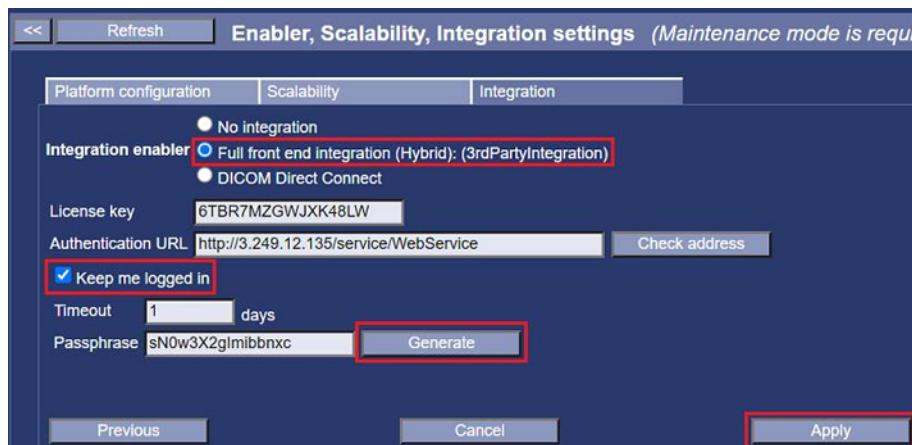
#### 7. **Full Front-End Integration(Hybrid): (3rd Party integration) option:**

##### **NOTE**

Hybrid integration is available for new installations, basic 3rd Party integration is only supported for AW Server 2.0 upgrades to AW Server 3.2.

Both types use the same license key.

If your site has purchased the option, and you have a "3rd Party integration license" key, click on **Full Front-End Integration(Hybrid): (3rd Party integration)**.



Enter the **License** key.

Enter the **Authentication URL**:

The "Authentication URL" is the URL link to the Web services of the remote system (subject to change. Refer to the PACS documentation):

Set the **Authentication URL** of the remote systems (CPACS, Universal Viewer,..., 3rd Party PACS) or leave the field blank if the remote systems do not implement this feature. Refer to the remote systems documentation for more information.

The following "Authentication URL" are given as examples for GE remote systems:

- **Authentication URL** for CPACS: [http://IMS\\_IP\\_address:9001/AWS/pacs/services](http://IMS_IP_address:9001/AWS/pacs/services)
- **Authentication URL** for Universal Viewer: [http://IUV\\_IP\\_address/services/PacsWebService](http://IUV_IP_address/services/PacsWebService)

**NOTE**

You can click on **Check address** button to check that the PACS system is alive.

**NOTE**

"3rd Party" PACS can be "synchronized" by the AW Server through Command lines. The "3rd Party" PACS vendor can use these Command lines to synchronize the AWS database with the PACS, referring to the AW Server 3.2 PACS Integration guide:  
**5535310-1EN**

**8. Optional step**

- a. Click on the **Keep me logged in** check box.
  - b. Select a number of days before connection is closed - typically 1 day.
  - c. Click on **Generate** button to automatically generate a *Passphrase* for connection security, or type in the *Passphrase* chosen by the user.
9. Click on the **Apply** button.

The message "Please reboot" will display.

You must reboot the AW Server now if you want to check that the integration is operational, or wait and continue with the other configuration steps and reboot later.

**NOTE**

To reboot, use the **Reboot** button from Service Tools/Utilities, or open a Terminal from Service Tools/Utilities, login as root and type in: reboot <Enter>

## 2.19.2.2 Configuration steps on the Universal Viewer

**NOTE**

Below are the steps to configure Hybrid integration with the Universal Viewer. This procedure is subject to change. Refer to the Universal Viewer documentation.

For other PACS systems, refer to the PACS documentation.

### 2.19.2.2.1 Install the Universal Viewer Server

1. Install the appropriate software release of Universal Viewer Server (PACS system).
2. Get the UV Installation/Upgrade Manual for the installed version at your site.
3. Also check GEHC Documentation Portal for the late version of that doc for that release.

### 2.19.2.2.2 Edit the integrations.ini file on the Client PC

It is necessary to indicate in the *integrations.ini* file the place where the AW Server Client is located.

1. Go to the UV Client folder: C:\Program Files (x86)\Integrad.3\MIV
2. Edit the file *integrations.ini*.
  - a. Find the section called "[HAWAII]"
  - b. Modify the line SOLO\_CLIENT\_PATH to look as follows: SOLO\_CLIENT\_PATH=C:\Program Files (x86)\GE\AWS\_3.2\solo

**NOTE**

Path might be different depending on the Windows configuration (32-bit/64-bit).

**NOTE**

When upgrading from AW Server 2.0 release, the path to integration.exe changes from AWS\_2.0 to AWS\_3.2

### 2.19.2.2.3 Configure Site Configuration Tool

1. Connect to the Universal Viewer Server and launch the Site Configuration Tool.
2. In "AW integration" menu, configure AW Configuration" tab as follows:
  - a. Check "**AWS 2.x Enable**"
  - b. Check "**Notification Enable**" if preprocessing is licensed and installed on AWS (optional).

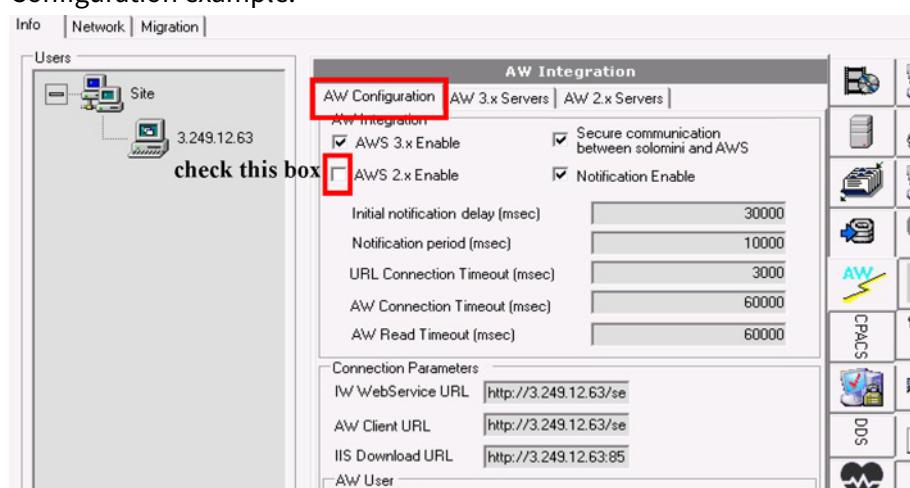
**NOTE**

If encryption is required for client-server communication using HTTPS, set it by checking "**Secure communication between solomini and AWS**" is reserved for Seamless integration.

- c. Fill the URLs with the Universal Viewer Server IP address:

- IW WebService URL: `http://<UV_IP_address>/services/PacsWebService`
- AW Client URL: `http://<UV_IP_address>/services/AWWebService`
- IIS Download URL: `http://<UV_IP_address>:85`

Configuration example:

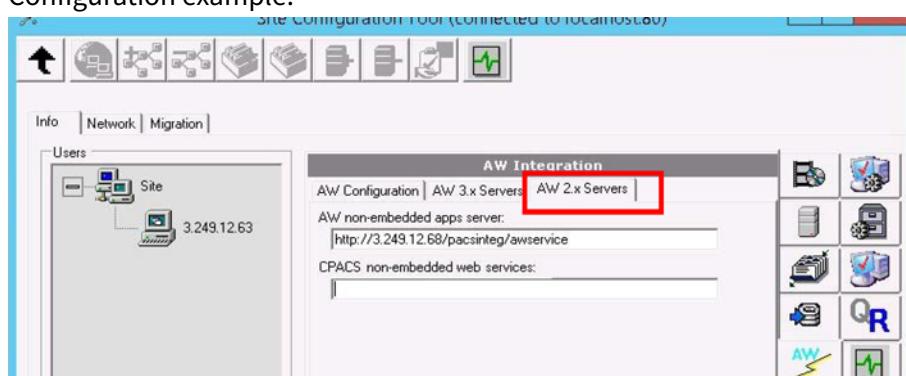


3. In "AW integration" menu, click on "**AW 2.x Servers**" tab and configure as follows:

Fill in IP address of the AW Server, and webservice:

- AW field: `http://<AW_Server_IP-address>/proxyservice/awservice`
- CPACS field: [`http://IMS\_IP\_address:9001/AWS/pacs/services`](http://IMS_IP_address:9001/AWS/pacs/services) (only applicable if CPACS backend)

Configuration example:



4. "Apply" site configuration parameters (nothing displays in red).
5. "Restart all "Integrad" services except the 2 SQL services.

### 2.19.2.2.4 Configuration of Universal Viewer users

UV users should have ADM group = AWS 2.

Refer to PACS documentation for details.

### 2.19.2.3 Configuration steps on the Client PC

The AW Server Client and the Universal Viewer Client must be installed on the PC.

Refer to the Universal Viewer documentation and to [2.24 Job Card IST014A - Standard Client PC installation & Tests on page 270](#) for the AW Server Client.

#### NOTICE

Do not select the *Client for Universal Viewer* (reserved for Seamless integration). Use *Client for Windows*.

## 2.19.3 Seamless Integration

This section details all the steps needed to configure the Seamless integration, in case of fresh installation, re-installation or upgrade.

#### For your information:

AW Server 3.2 Installation Manual refers to the current Universal Viewer Installation and service documentation for integration details on the UV side.

Get the UV Installation/Upgrade Manual for the installed version at your site.

#### NOTE

Also check GEHC Documentation Portal for the latest version of the docs for that release.

#### NOTE

In this document, the expression Universal Viewer Server refers to the Universal Viewer Workflow Manager. Other components of Universal Viewer are explicitly mentioned when needed.

### 2.19.3.1 Pre-requisites summary

#### Database

Seamless integration is using the PACS database, so AW Server does not contain images (apart from reconstruction images generated on the AW Server that will be pushed to the PACS by the End of Review feature).

#### Software license key

A software license key is required to enable Integration between the AW Server and the GE PACS. The license key is based on the following keystring: *Seamless\_Integration*.

#### Seamless connector plugin media (Dakota plugin media)

This client software library is delivered with the Universal Viewer / GE PACS for "Seamless" integration. It must be loaded on the AW Server to enable "Seamless" integration with the PACS. Currently, for the Universal Viewer, it is delivered as a RPM file on a media.

#### For information:

A similar plugin is delivered with the CPACS to enable "Full Frontend & Backend" integration with the CPACS.

The installation and setup procedure of this seamless connector plugin is explained in the section [2.19.3.4 Seamless integration - configuration steps on AWS, Service Tools on page 231](#) "Seamless integration configuration steps on AWS, Service Tools" below.

### Universal Viewer Server

The Universal Viewer Server shall be installed and configured. See [2.19.3.2 Seamless integration - configuration steps on Universal Viewer Server on page 229](#)

## 2.19.3.2 Seamless integration - configuration steps on Universal Viewer Server

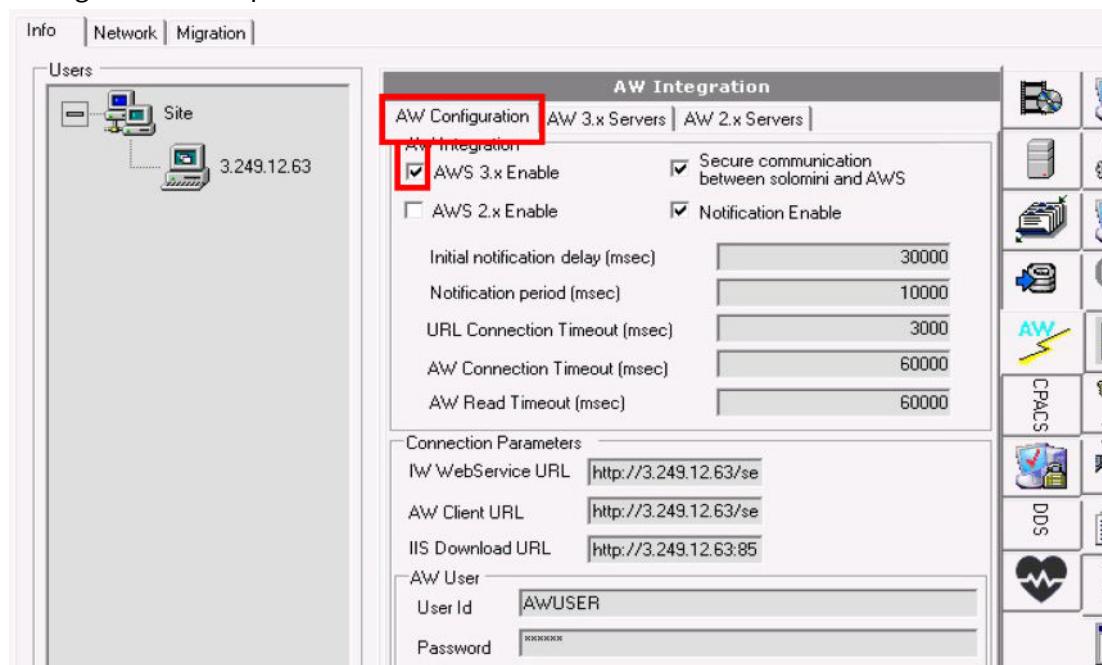
### 2.19.3.2.1 Install the Universal Viewer Server

- 1.)  • Install the appropriate software release of Universal Viewer Server (PACS system).
  - Get the UV Installation/Upgrade Manual for the installed version at your site.
  - Also check GEHC Documentation Portal for the late version of that doc for that release.
- 2.)  • On the Universal Viewer Server, check that there is a file **FetchUpNewAWSClient.vbs** in the folder **C:\Integrad\Current\bin**.

### 2.19.3.2.2 Configure Site Configuration Tool

1. Connect to the Universal Viewer Server and launch the Site Configuration Tool.
2. In "AW integration" menu, configure AW Configuration tab as follows:
  - a. Check "**AWS 3.x Enable**"
  - b. Check "**Notification Enable**" if preprocessing is licensed and installed on AWS (optional). If encryption is required for client-server communication using HTTPS, set it by checking "**Secure communication between solomini and AWS**".
  - c. Fill the URLs with the Universal Viewer Server IP address:
    - IW WebService URL: `http://<UV_IP_address>/services/PacsWebService`
    - AW Client URL: `http://<UV_IP_address>/services/AWWebService`
    - IIS Download URL: `http://<UV_IP_address>:85`

Configuration example:



AW User: Indicate a user and its password in "User Id" and "Password". For example, the recommended login/password in Universal Viewer Install Manual is: **AWDakota** .

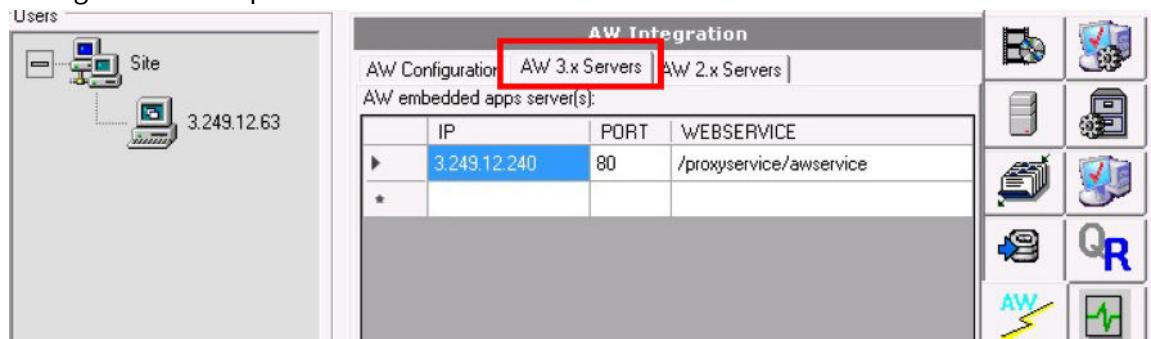
(In our example snapshot, we used "AWUSER")

3. In "AW integration" menu, click on "**AW 3.x Servers**" tab and configure as follows:

Fill in IP address of the AW Server, port **80** and webservice: <AW Server\_IP-address>/proxyservice/awservice

If several AW Servers are integrated with the Universal Viewer Server, indicate each AW Server in a separate row.

Configuration example:



4. "Apply" site configuration parameters (nothing displays in red).
5. "Restart all "Integrad" services except the 2 SQL services.

### 2.19.3.2.3 Create an AW Server user

1. Connect to the administration of Universal Viewer Server in an internet browser by entering the following IP address: `http://<IP of the Universal Viewer Server>/admin`
2. Create an AW User named for example **AWDakota**.
3. Configure *ADM Group* with Digital Imaging, Administrator and AWS 3, and configure *Institution* for this user.
4. If the site has purchased the *Pre-processing* option, create an Pre-processing user named for example **AWPreProc** with same password as **AWDakota**.

### 2.19.3.2.4 Configuration of Universal Viewer users

UV users should have ADM group = AWS 3.

Refer to PACS documentation for details.

### 2.19.3.2.5 Add Virtual Drive and Create MIME Type

In the Server Manager:

1. Add a virtual drive named "storage" with path "**C:\Integrad\Current\Data**"
2. Add two MIME types "**dcm**" and "**jp2**"

Refer to the Universal Viewer Installation Manual for more details.

## 2.19.3.3 Seamless integration - configuration steps on AWS

### DNS

DNS must be configured to fit the site's parameters. Refer to [2.13 Job Card IST005 - Network and Time Configuration on page 127](#) and/or [A.8 Useful Commands and Tools on page 589](#). This is necessary to ensure that the AW Server will be able to connect to the different Universal Viewer systems.

### Auto Delete

Configure the Auto Delete feature so that local images are purged, for example after one day.

Refer to [2.15.7 Database Deletion Settings on page 150](#): Auto Delete.

### DICOM Host

The RIS or PACS system shall be properly declared as a DICOM Host in AW Server. Detailed instructions are available in [2.18 Job Card IST010 - Administrative Configuration on page 184](#).

### NOTICE

The Universal Viewer can have 2 different type of back-end: IW back-end or CPACS back-end.IW back-end case: for single server installation, declare the Workflow Manager (which is also the back-end). For large installation, declare the IW back-end as a DICOM host.CPACS back-end case: declare the CPACS DAS as a DICOM host.

- When configuring DICOM information for PACS Query Retrieve, **Allow Query**, **Allow Retrieve**, **Allow Store** shall be enabled.
- PACS systems supporting Storage Commitment shall be configured on the AW Server.

### End Of Review

End of Review must be configured with the DICOM host declared in the previous step "DICOM host configuration". Detailed instructions are available in [2.18.10 End of Review on page 210](#)

- The Seamless Integration (if applicable to your site) shall be fully configured before configuring End of Review.
- The TYPE of images to be sent to the PACS system when configured shall be set to "generated".
- All modality image types shall be enabled, unless the receiving PACS system does not support a particular image type, then do not select this type of image.

### Pre-processing

It is not mandatory to configure Pre-processing when integrating to PACS, but it would improve the perceived performance. Refer to [2.15.10 Licensing Configuration on page 156](#)

- AW Server requires a software license key to enable the Pre-processing feature.
- If used in cluster mode, all AW servers shall have enabled and licensed Preprocessing. Additionally, the same setup must be configured on each server (enable preprocessing for the same set of applications, use the same series descriptor).

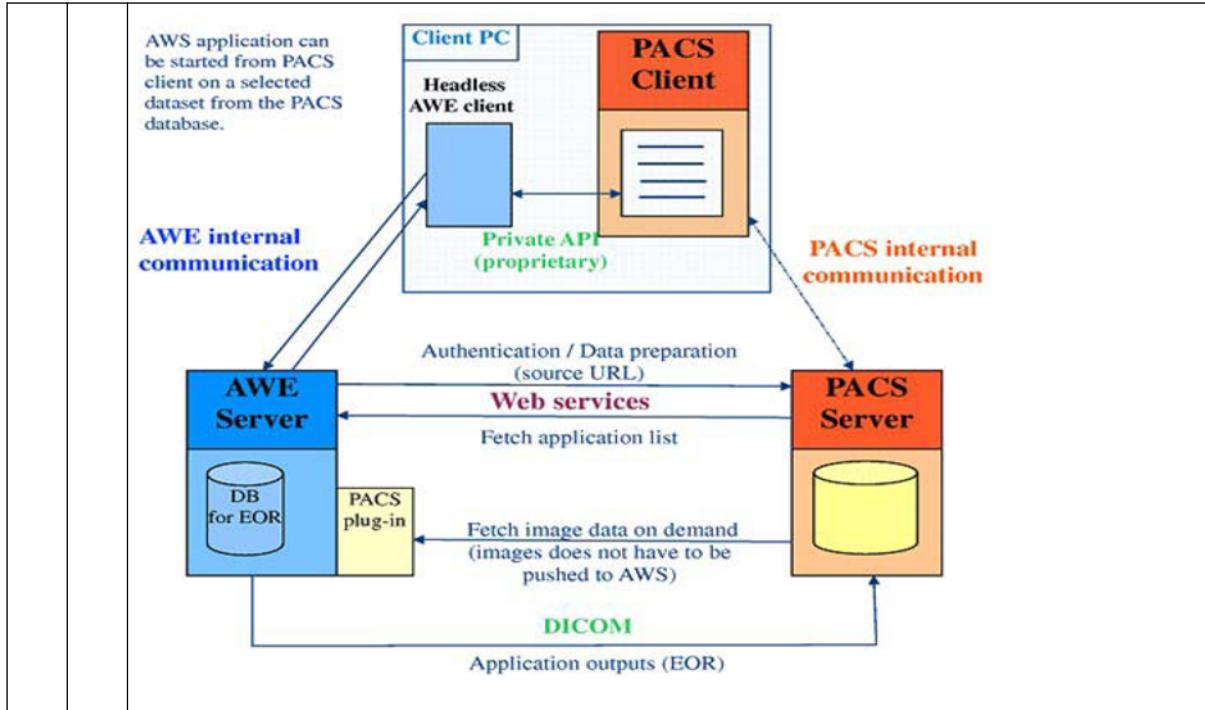
### Seamless connector plugin (Dakota plugin)

See next section.

## 2.19.3.4 Seamless integration - configuration steps on AWS, Service Tools

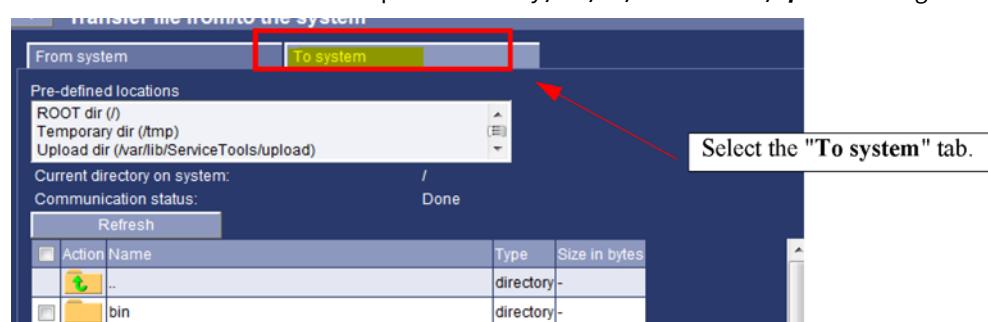
By default the Server is in Standalone (Non-Integrated) mode. Only execute the following procedure if you have to configure the Seamless Integration.

Please refer to the PACS documentation for detailed information on the UV's settings.

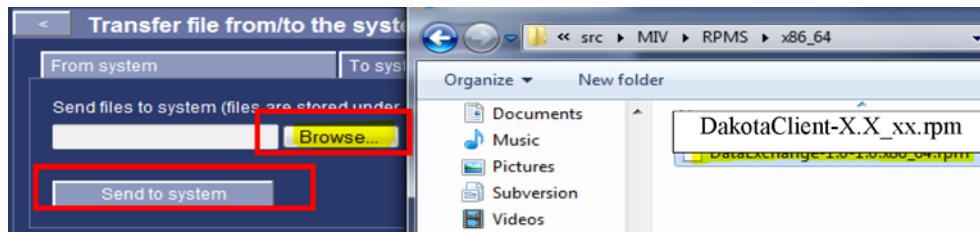


### 2.19.3.4.1 Dakota plugin installation steps

- 1.) • Make sure the AW Server is still in Maintenance mode or place it under **Maintenance**. Refer to [A.4 Maintenance Mode on page 571](#) for details.
- 2.) **Dakota plugin installation.**
  - From **Service Tools /Tools** menu, open the **Terminal** and login as **root**.
  - Check for the eventual presence of an older Dakota package, and if present, remove it prior to load the one delivered with your PACS system.
    - Check for a Dakota package  
**rpm -qa | grep Dakota <Enter>**
    - If a package is present, remove it now  
**rpm -e Dakota\* <Enter>**
- 3.) • If the Dakota plugin is delivered as part of a media (CD or USB device for example), insert the media containing the Dakota plugin package into the DVD drive or a USB port of the Client PC.
- 4.) • Load the PACS Connector "Dakota" Plugin from the SW media (or link) delivered with the PACS.
  - From the **Tools** menu, select the **File Transfer tool** in order to load the *DakotaClient-X.X\_xx.rpm* package to the server. I.e: DakotaClient-5.x86\_64.rpm
  - Select the **To system** tab
  - Browse to the DVD drive or USB device of the Client PC or local repository where you have previously stored the plugin.
  - Select the Dakota client
  - Select the standard Service Tools Upload directory **/var/lib/ServiceTools/upload** as target.



- 5.)
  - Click the '**Browse**' button and choose the rpm to deploy from your local machine, for example:
  - Click on **Send to system** button:



A message confirms the successful upload.

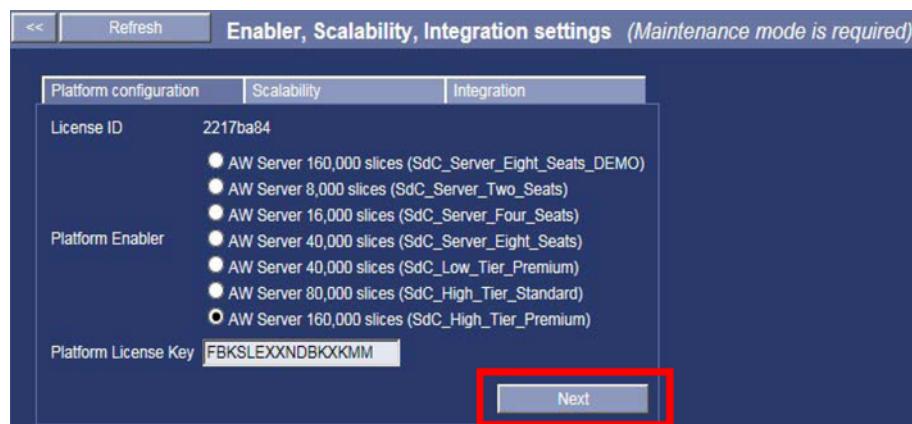
- 6.)
  - Install the PACS "Dakota" Connector plug-in on the AW Server:
    - From the Service Tools menu, select **Tools > Terminal**, if not done yet.
    - Login as **root** and execute the following commands to double-check the upload is present:  
`cd /var/lib/ServiceTools/upload <Enter>`  
`ls -ltr <Enter>`  
I.e: `-rw-r--r-- 1 tomcat tomcat 85259662 Jul 24 15:20 DakotaClient-5.x86_64.rpm`
    - Enter the following command in the Terminal window to install the package:  
`rpm -Uvhf DakotaClient-X.X_xx.rpm <Enter>` (where X.X\_xx is the package release number)  
I.e: `rpm -Uvhf DakotaClient-5.x86_64.rpm`

#### NOTICE

Always use the latest available Dakota plugin. Refer to the PACS documentation for the latest available plugin.

### 2.19.3.4.2 Seamless Integration setup steps

- 1.)
    - From the Service Tools menu, click on **Initial Configuration** to expand the menu.
  - 2.)
    - Click on **Platform Configuration**.
- The following menu displays:



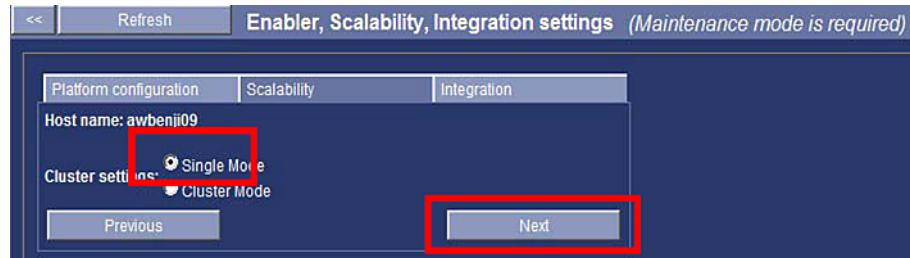
Refer to [2.15.9 Platform Configuration on page 153](#) for details.

- 3.)
  - Make sure the “Platform Enabler” license has been entered. If not, enter it now.
  - When done, click on the **Next** button to change to the **Scalability** tab.

**4.) Scalability: Virtual AW Server to be placed into a cluster of virtual AW servers:**

- If your AW Server shall be part of a cluster of virtual AW Servers, the Cluster mode radio button must be checked.

You will be prompted to enter the IP address of the two HAPS server nodes.



If applicable for your site, Scalability configuration shall be done as part of [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

- When done, click on the **Next** button to change to the *Integration* tab

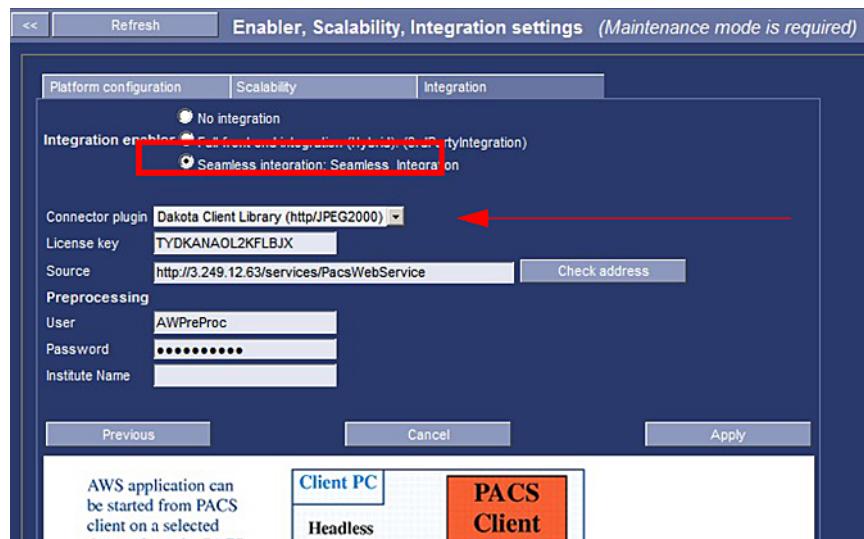
**5.) Now you can setup integration**

- Go back to the Service Tools / **Platform Configuration** menu:

Refer to [2.15.9 Platform Configuration on page 153](#) for details.

- Click on **Platform Configuration** sub-menu, and directly click on the **Next** button
- Click on **Scalability** sub-menu, and directly click on the **Next** button

The Integration sub-menu displays:



- **Integration Enabler:**

Select **Seamless integration** check box and enter the parameters as shown hereafter:

- 6.)
- **Connector plugin:**  
Select the **Dakota Client Library** plugin from the pull down menu
  - **License key:**  
Enter the license key for Seamless Integration  
(keystring : Seamless\_Integration)
  - **Source:**  
***http://<IP address of UniversalViewer\_server>/services/PacsWebService***
- NOTE**
- Enter the IP address of the Universal Viewer Workflow Manager Controller (regardless of the type of back-end used: IW or CPACS)
- **Preprocessing user:**  
It is an Universal Viewer user (in our example, we use the default AWPreProc user). For the preprocessing User and Password, enter valid values for a Universal Viewer Database preprocessing.
  - **Institute Name:** Enter the hospital name or any other suitable information.
    - If you are using CPACS integration, leave this field blank.
    - If you are not using CPACS integration, enter the institution name of the Universal Viewer Database server.
- 7.)
- Now click on **Apply** to enable the Seamless integration configuration.  
The following confirmation messages display when the integration mode is applied:
- All the DICOM data stored in the database will be deleted !***
- It is strongly recommended to transfer the data to a remote system.***
- Please contact the IT Admin and check which images need to be saved on PACS. Do you want to continue the configuration now ?***

### NOTICE

If this is a new installation, no images are present in the AW Server database. In case of upgrade, make sure with your customer that all image data has previously been stored on another system prior to continue.

- Click **OK** to acknowledge.

The following popup message displays:

***All the DICOM data stored in the database will now be deleted !***

***Do you want to proceed with the configuration now ?***

- Click **OK** to acknowledge.

***Please reboot the system***

- Click on **OK** to acknowledge the message.

- 8.)
- Prior to reboot your system, verify that Exam series images will be loaded using the Dakota client plugin:. In the Terminal window type:
    - **cd /export/home/sdc/integration/plugindata <Enter>**
    - **ls -ltr <Enter>**

The softlink 'current' should point to Dakota Client as shown in the example below.

```
btn:/export/home/sdc/integration/plugindata # ls -ltr
al 8
xr-xr-x 4 sdc  sdc  4096 Aug 16 18:46 IWPlugin
xr-xr-x 4 root  root  4096 Aug 16 21:58 DakotaClient
rwxrwx 1 root  root   52 Aug 16 22:07 current -> /export/home/sdc/integration/plugindata/DakotaClient
btn:/export/home/sdc/integration/plugindata #
```

- 9.)
  - Reboot the server now  
OR  
proceed to the other features configuration steps first, then you will shutdown and reboot when the other configuration steps are done.
  - When done, in the Terminal window type:
    - **reboot <Enter>**
- 10.)
  - Now you can configure the **End Of Review** feature.  
Refer to [2.18.10 End of Review on page 210](#)

### 2.19.3.5 Seamless integration - configuration steps on Universal Viewer Client PC

AWS Integrated Client will be installed later as part of [2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282](#)

Do not install it now.

### 2.19.3.6 Seamless integration - configuration steps on Image Sources

Image Database:

Modalities shall be set to **auto-push** images to the PACS.

### 2.19.3.7 Seamless Integration - configuration checklist

This section intends to provide a high level checklist of all steps required for seamless integration on each system: AW Server, Universal Viewer Server, Universal Viewer Client PC. This can be used as a troubleshooting help to ensure that no steps were missed during the configuration.

#### 2.19.3.7.1 On the AW Server side

Step	Check	Action	On	Further details, refer to:
1.)	<input type="checkbox"/>	<b>DNS</b> is configured as part of Network configuration	AW Server	<a href="#">AWS IM, 2.13 Job Card IST005 - Network and Time Configuration on page 127</a>
2.)	<input type="checkbox"/>	<b>Auto-delete</b> is enabled	AW Server	<a href="#">AWS IM, 2.15 Job Card IST008 - Initial Configuration on page 140</a>
3.)	<input type="checkbox"/>	The <b>Universal Viewer Server</b> is properly declared as a DICOM Host in AW Server (2 cases: IW back-end and CPACS back-end)	AW Server	<a href="#">AWS IM, 2.18 Job Card IST010 - Administrative Configuration on page 184</a>
4.)	<input type="checkbox"/>	Optional step: <b>Pre-processing</b> is configured. Preprocessing license is entered.	AW Server	<a href="#">AWS IM, 2.15 Job Card IST008 - Initial Configuration on page 140</a>
5.)	<input type="checkbox"/>	The " <b>Dakota</b> " Integration plugin has been loaded from the media and is installed on AWS	AW Server	<a href="#">AWS IM, 2.19 Job Card IST011 - Integration on page 221 ; 2.15 Job Card IST008 - Initial Configuration on page 140</a>
6.)	<input type="checkbox"/>	The " <b>Seamless</b> " software license key is entered to enable the Integration mode	AW Server	<a href="#">AWS IM, 2.19 Job Card IST011 - Integration on page 221 ; 2.15 Job Card IST008 - Initial Configuration on page 140</a>
7.)	<input type="checkbox"/>	The <b>Dakota Library</b> item is selected in the <b>Connector plugin</b> drop-down list.	AW Server	<a href="#">AWS IM, 2.19 Job Card IST011 - Integration on page 221 ; 2.15 Job Card IST008 - Initial Configuration on page 140</a>

<b>Step</b>	<b>Check</b>	<b>Action</b>	<b>On</b>	<b>Further details, refer to:</b>
8.)	<input type="checkbox"/>	The PACS web service URL is entered in the <b>Source</b> field.	AW Server	AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
9.)	<input type="checkbox"/>	Preprocessing parameters are entered (user, password, Institution) if applicable	AW Server	AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
10.)	<input type="checkbox"/>	AW Server has been rebooted to take into account the Integration configuration.	AW Server	AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a> ; <a href="#">2.15 Job Card IST008 - Initial Configuration on page 140</a>
11.)	<input type="checkbox"/>	<b>End of Review</b> is configured	AW Server	AWS IM, <a href="#">2.18 Job Card IST010 - Administrative Configuration on page 184</a> ,

### 2.19.3.7.2 On Universal Viewer Server

<b>Step</b>	<b>Check</b>	<b>Action</b>	<b>On</b>	<b>Further details, refer to:</b>
1.)	<input type="checkbox"/>	Universal Viewer Server is installed	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
2.)	<input type="checkbox"/>	<i>In Site Configuration Tool / AW Configuration</i> tab is configured	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
3.)	<input type="checkbox"/>	<i>In Site Configuration Tool / AW Servers</i> tab is configured with one or several servers.	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
4.)	<input type="checkbox"/>	An AW Server user is created in Universal Viewer (e.g "AWDakota")	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
5.)	<input type="checkbox"/>	A preprocessing user is created in Universal Viewer (e.g "AWPreproc")	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
6.)	<input type="checkbox"/>	Universal Viewer users have the AWS 3 group.	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>
7.)	<input type="checkbox"/>	Virtual Drive is added and 2 MIME Types are created	Universal Viewer Server	<b>Universal Viewer IM</b> and AWS IM, <a href="#">2.19 Job Card IST011 - Integration on page 221</a>

### 2.19.3.7.3 On Universal Viewer Client PC

<b>Step</b>	<b>Check</b>	<b>Action</b>	<b>On</b>	<b>Further details, refer to:</b>
1.)	<input type="checkbox"/>	Universal Viewer (IW) Client is installed on the RIS/PACS workstations where integration will be used by the customer.	Universal Viewer Client PC	<b>Universal Viewer IM</b> and <a href="#">2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282</a>
2.)	<input type="checkbox"/>	AWS Client is installed on the Universal Viewer Server.	Universal Viewer Client PC	<b>Universal Viewer IM</b> and <a href="#">2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282</a>

Step	Check	Action	On	Further details, refer to:
3.)	<input type="checkbox"/>	In Universal Viewer Client, 3D applications button is configured	Universal Viewer Client PC	<a href="#">Universal Viewer IM</a> and <a href="#">2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282</a>
4.)	<input type="checkbox"/>	AWS Client is installed on the Universal Viewer Client workstations where integration will be used by the customer.	Universal Viewer Client PC	<a href="#">Universal Viewer IM</a> and <a href="#">2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282</a>

### 2.19.3.7.4 On the Image sources

Step	Check	Action	On	Further details, refer to:
1	<input type="checkbox"/>	Modalities are set to auto-push images to the PACS.	Image Sources	Image Source documentation

## 2.19.4 DICOM Direct Connect integration

This section details all the steps needed to configure the DICOM Direct Connect integration, in case of new installation, re-installation or upgrade.

DICOM Direct Connect is currently supported on **Virtual AW Server Low Tier only** (40K slices) only. The clustering mode (Scalability) is also supported.

#### NOTE

For AW Server running in CT Console environment (NanoCloud AW Server), refer to the current Modality console Installation and service documentation for integration details on the Modality console side.

#### NOTE

Also check the Documentation Portal for the latest version of the docs for that release.

### 2.19.4.1 Pre-requisites

#### Database

DICOM Direct Connect integration is using the PACS, VNA or any DICOM Remote Hosts database, so AW Server does not contain images (apart from images generated on the AW Server that will be pushed to the PACS/VNA/DICOM Remote Hosts by the End of Review functionality).

#### Software license key

A software license key is required to enable integration between the AW Server and the PACS/VNA/DICOM Remote Hosts. The license key is based on the following keystring: *DICOM\_Direct\_Connect*.

#### DICOM Host definition

The AW Server shall be declared twice in the PACS/VNA/DICOM Remote Hosts system. Refer to section [2.19.4.4 Configuration steps on the PACS/VNA/DICOM Remote Host on page 242](#).

### 2.19.4.2 Configuration steps on AWS

#### DNS

DNS must be configured to fit the site's parameters. Refer to [2.13 Job Card IST005 - Network and Time Configuration on page 127](#) and/or [A.8 Useful Commands and Tools on page 589](#). This is necessary to ensure that the AW Server will be able to connect to the different PACS/VNA/DICOM Remote Host systems.

#### Auto Delete

Configure the Auto Delete feature so that local images are purged, for example after one day.

Refer to [2.15.7 Database Deletion Settings on page 150](#): Auto Delete.

### DICOM Host

The PACS/VNA/DICOM Remote Host system shall be properly declared as a DICOM Host in AW Server. Detailed instructions are available in [2.18 Job Card IST010 - Administrative Configuration on page 184](#).

Refer to PACS/VNA/DICOM Remote Host documentation for host characteristic.

- **Allow Query, Allow Retrieve, Allow Store** shall be enabled if the DICOM Host supports the Query Retrieve function.
- **Storage Commitment** shall be enabled if the DICOM Host is a PACS supporting this function.

### End Of Review

End of Review must be configured with the DICOM hosts declared in the previous step “DICOM host”. Detailed instructions are available in [2.18.10 End of Review on page 210](#)

- The DICOM Direct Connect Integration shall be fully configured before configuring End of Review.
- The TYPE of images to be sent to the PACS/VNA system when configured shall be set to “generated”.
- All modality image types shall be enabled, unless the receiving PACS/VNA system does not support a particular image type, then do not select this type of image.

### Preprocessing

Preprocessing is not mandatory, but it improves productivity by preprocessing data before the user opens an exam. Refer to [2.15.10 Licensing Configuration on page 156](#).

AW Server requires a software license key to enable the Preprocessing feature.

In cluster mode, Preprocessing shall be licensed and enabled on all AW server nodes and the preprocessing protocols shall be configured (**Service Tools/Administrative/Configuration/Preprocessing**) with the same series descriptors.

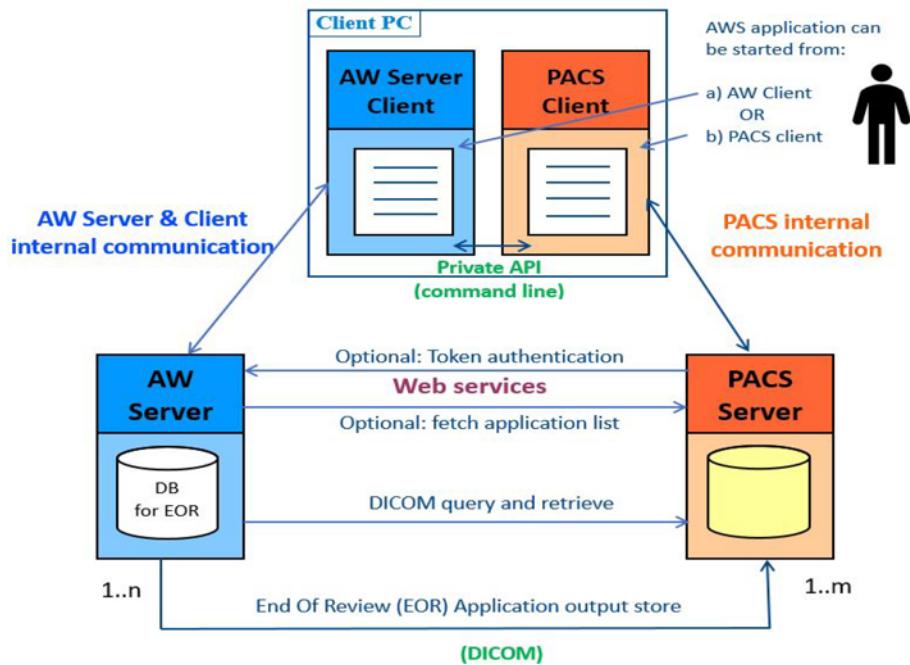
#### NOTE

In DICOM Direct Connect integration mode, the PACS/VNA/DICOM Remote Host system must be configured to send DICOM Instance Availability Notifications (IAN) to the AW Server (to the first node in case of a cluster). Refer to [2.18.8 Preprocessing Configuration on page 204](#).

## 2.19.4.3 Configuration steps on AWS, Service Tools

By default the Server is in Standalone (Non-Integrated) mode.

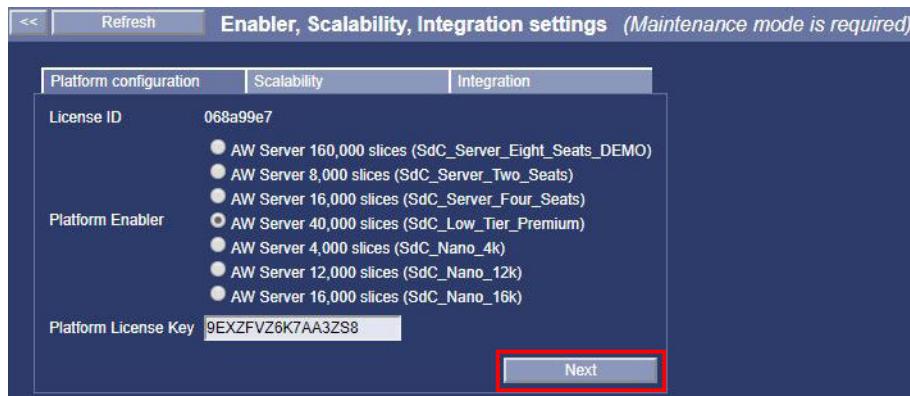
Only execute the following procedure if you have to configure the DICOM Direct Connect Integration.



### 2.19.4.3.1 DICOM Direct Connect Integration setup steps

1. If not already done, put the AW Server in **Maintenance** mode. Refer to chapter 4, [A.4 Maintenance Mode on page 571](#) for details.
2. From the Service Tools menu, click on **Initial Configuration** to expand the menu.
3. Click on **Platform Configuration**.

The *Platform configuration* tab displays:



Refer to [2.15.9 Platform Configuration on page 153](#) for details.

#### 4. Platform Configuration:

- Select the **Platform Enabler** license **AW Server 40,000 slices (SdC\_Low\_Tier\_Premium)**

#### NOTE

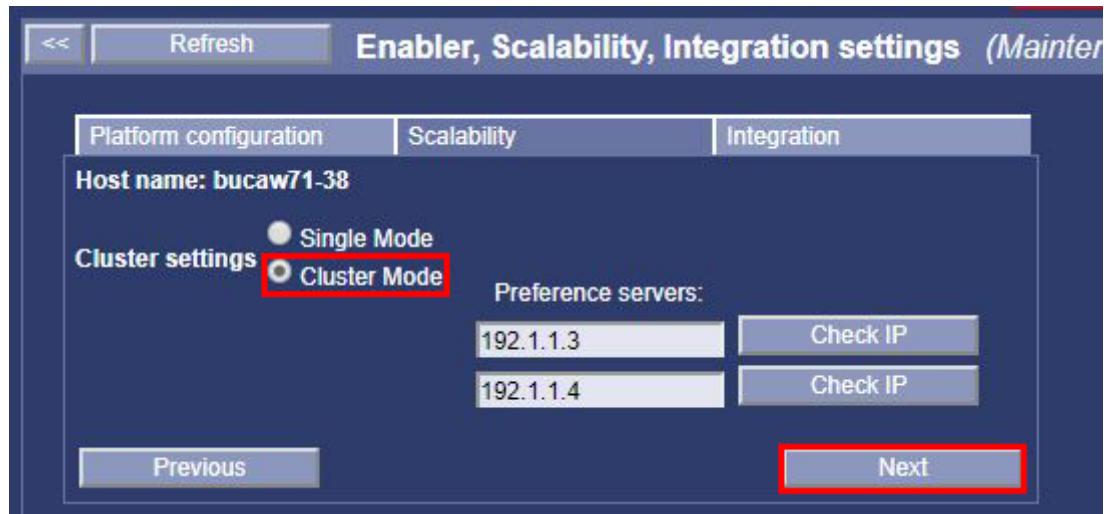
For AW Server running in CT Console environment (NanoCloud AW Server), select one of the **SdC\_Nano\_nk** license and enter the corresponding Platform License Key. Refer to the current Modality console Installation and service documentation.

- Enter the **Platform License key** for **SdC\_Low\_Tier\_Premium** in the text field.
- Click **Next** button to change to the *Scalability* tab.

#### 5. Scalability: Virtual AW Server to be placed into a cluster of virtual AW servers:

- If your AW Server shall be part of a cluster, select the **Cluster Mode**.

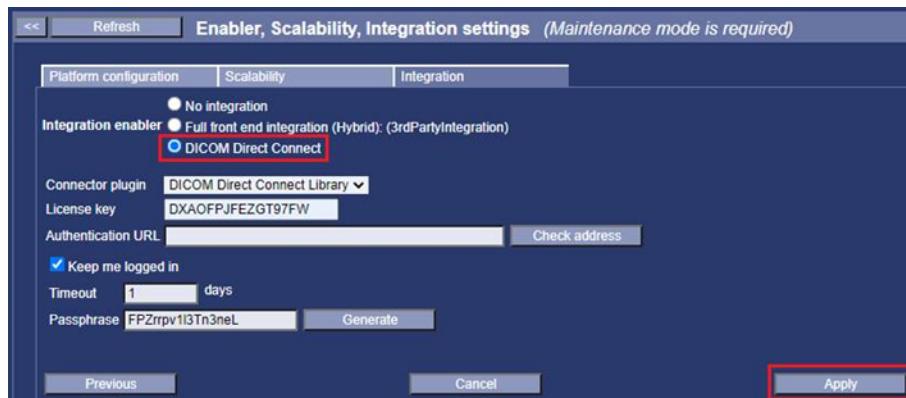
In that case, enter the IP address of the two HAPS (High Availability Preference Server) nodes.



If applicable for your site, Scalability configuration shall be done as part of [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

- When done, click on the **Next** button to change to the *Integration* tab

## 6. The Integration sub-menu display:



## 7. Integration steps:

- **Integration Enabler:**

Select the **DICOM Direct Connect** radio button.

- **Connector plugin:**

**DICOM Direct Connect** plugin is selected.

- **License key:**

Enter the license key for DICOM Direct Connect Integration  
(keystring : *DICOM\_Direct\_Connect*)

- **Authentication URL:**

The “Authentication URL” is only needed if PACS/VNA front-end client integration is used.  
Refer to the PACS/VNA/DICOM Remote Host documentation.

## 8. Optional steps:

- Click on the **Keep me logged in** check box.

- Select a number of days before connection is closed - typically 1 day.
  - Click on **Generate** button to automatically generate a *Passphrase* for connection security, or type in the *Passphrase* chosen by the user.
9. Now click on **Apply** to enable the DICOM Direct Connect integration configuration.

The following confirmation messages display when the integration mode is applied:

***All the DICOM data stored in the database will be deleted !***

***It is strongly recommended to transfer the data to a remote system.***

***Please contact the IT Admin and check which images need to be saved on PACS. Do you want to continue the configuration now ?***

#### **NOTICE**

If this is a new installation, no images are present in the AW Server database. In case of upgrade, make sure with your customer that all image data has previously been stored on another system before continuing.

- Click **OK** to acknowledge.

The following popup message displays:

***All the DICOM data stored in the database will now be deleted !***

***Do you want to proceed with the configuration now ?***

- Click **OK** to acknowledge.

***Please reboot the system***

- Click on **OK** to acknowledge the message.

10. Reboot the server now

OR

proceed to the other features configuration steps first, then you will shutdown and reboot when the other configuration steps are done.

To reboot, from the Service Tools menu:

- Click on **Tools** to expand the menu.
- Then click on **Reboot**.
- In the left panel, click on the **Reboot AW Server** button.

### **2.19.4.4 Configuration steps on the PACS/VNA/DICOM Remote Host**

For each AW Server node you have to declare the AW Server host twice in the PACS/VNA/DICOM Remote Host:

- One entry with the <host name>/<AET>, IP and port **4006** for standard DICOM functions.
- The second entry with <host name>**\_ds**/<AET>**\_ds**, same IP and port **4010** for DICOM Direct Connect.

#### **2.19.4.4.1 Configuration steps on Enterprise Archive (EA)**

This section describes the steps to declare the AW Server in the Enterprise Archive (EA).

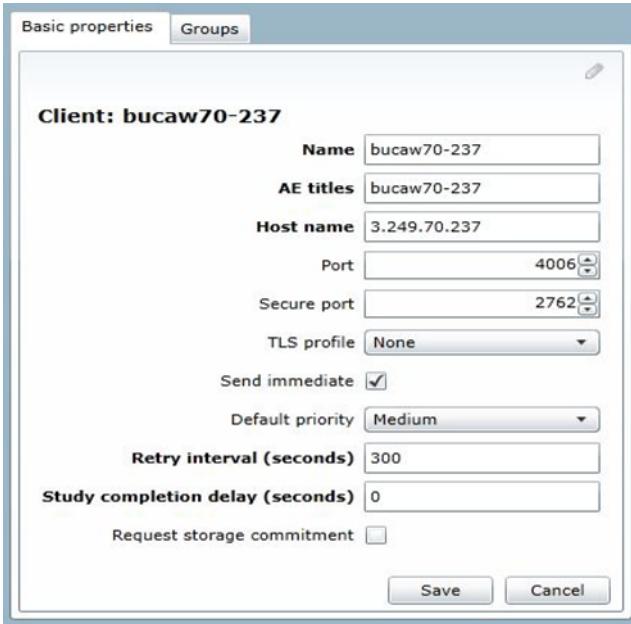
1. Connect to the Enterprise Archive Server Web page URL with:

EA Web Service URL: **[http://<EA\\_IP\\_address>/eaconsole](http://<EA_IP_address>/eaconsole)**

## NOTICE

Enterprise Archive Server Web page may not be properly working in Chrome and Firefox web browsers. Preferably use IE.

2. From the Enterprise Archive Server Web main page, login as **Administrator**. Refer to the EA administrator for more details on how to require EA access.
3. On the left hand side menu, click on **Communication** to expand the menu. Then select **DICOM clients**.
4. Click on the **New** button. The right part of the interface allows you to declare the AWS.



5. Fill in the fields as follow (note that the AWS HealthPage displays the needed information):
  - Enter the host name in the **Name**, field.
  - Enter the Application Entity Title (AET) in the **AE titles** field.
  - Enter the IP Address in the **Host name** field.
  - Enter the port number in the **Port** field.

### NOTE

Refer to the EA administrator if other fields need to be addressed.

## 2.19.4.5 Configuration steps on the Client PC

The AW Server Client and the PACS Client must be installed on the PC.

Refer to the PACS documentation and to [2.24 Job Card IST014A - Standard Client PC installation & Tests on page 270](#) for the AW Server Client.

### NOTE

For AW Server running in CT Console environment (NanoCloud AW Server), AWS Client will be integrated within the CT Console Client. Refer to CT documentation for full description.

### **DICOM Direct Connect Integration configuration is complete.**

For additional information to setup the whole cluster, refer to [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

OR

**Proceed to [2.22 Job Card IST013 - System Configuration Registration on page 259](#)**

## 2.20 Job Card IST012 - Virtual Servers Cluster Configuration

### 2.20.1 Foreword

Scalability mode (or cluster mode) is the ability to have several AW Servers working as one more powerful AW server (currently limited to a maximum of “virtual” AW Servers). The behavior is “transparent” for the user, who will be automatically directed to the appropriate server (less loaded) when logging in.

If your site is going to have a cluster of two or more virtual AW servers, you need to set up each of the servers in the "Cluster mode". Proceed as follows and repeat this operation on each of the other virtual AW servers.

**Currently, the Scalable mode is only supported with virtual AW Servers.**

#### NOTICE

Pre-requisite to performing this Job Card is the successful completion of: [2.8 Job Card IST001C - Virtual Servers Cluster Installation Steps on page 80](#) and [2.19 Job Card IST011 - Integration on page 221](#).

### 2.20.2 Certificate Management

In order for the nodes (AW Servers) and the HAPS to communicate securely between them, we need to generate public/private keys and certificates and deploy them on the nodes and the HAPS.

This operation is performed on **one node** and propagate to all the nodes of the cluster.

1. Choose one node that will be the "certificate provider".

Open a **Terminal** from the **Tools** menu and login as **root**.

2. Create a configuration file containing the internal IP addresses of all the nodes and the two HAPS of the cluster:

For each node/HAPS IP address, type the command:

**echo -e <NODE\_IP> >> /root/nodes.cfg <Enter>**

For instance: **echo -e 3.249.12.241 >> /root/nodes.cfg**

3. Check the content of the /root/nodes.cfg file:

Type the following command:

**cat /root/nodes.cfg <Enter>**

For a cluster of 3 nodes, the result of the command should be (provided that the node IP addresses entered in previous point are: 3.249.12.241, 3.249.12.242 and 3.249.12.243 and the HAPS IP addresses entered in previous point are: 3.249.12.251 and 3.249.12.252):

3.249.12.241

3.249.12.242

3.249.12.243

3.249.12.251

3.249.12.252

4. Generate the certificates:

Type the following command:

**/root/certificate-management/awsCert generate <Enter>**

This command return the passphrase of server's key, note it down.

5. Apply the certificates:

Execute next steps for each node and the two HAPS of the cluster:

**NOTE**

Execute the steps first on HAPS with lower IP and after that on HAPS with higher IP.  
Then on the nodes indefferently.

- Open a **Terminal** and login as **root**.
- Apply the certificate by running the following command:

**/root/certificate-management/awsCert apply <Provider\_IP> <Enter>**

<Provider\_IP> is the IP of the "certificate provider" node (see step 1).

For instance: **/root/certificate-management/awsCert apply 3.249.70.241**

The command will request a passphrase. Enter the passphrase noted down in previous step.

- For the HAPS, verify that the 3 following services are running:

Type in the following commands:

**systemctl status hws-service glusterd clb-service <Enter>**

You should see 3 times (once for each service) the following line within the result of the command:

*Active: active (running) since...*

## 2.20.3 Scalability setup procedure

### 2.20.3.1 NTP server availability checks

1. Time synchronization through a NTP server is a "must be" for scalability.

Check on each AW Server that the NTP server is operational.

- Open the **Terminal** from the **Tools** menu and login as **root**.
- Type in the Terminal:

**systemctl status chronyd <Enter>**

*Active: active (running) since...*

2. If no NTP server displays, ask the IT admin of the site to provide you with a NTP server IP address, and refer to section [2.15.6.2 Time Server menu on page 149](#) to setup the NTP server.

### 2.20.3.2 Scalability setup

#### 2.20.3.2.1 Scalability mode setup

1. From the **Service Tools / Initial Configuration** menu:

- Click on **Platform configuration**.

The configuration tool opens on Platform configuration tab.

- Make sure the Platform License key has been entered. If not done, refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#) to set it up.
  - Click on **Next** to move to *Scalability* tab.
2. Scalability mode setup
- Check that the **Cluster Mode** radio button is selected, or select it if not done.
  - Enter the **IP address** of HAPS Preferences server 1# and **IP address** of HAPS Preferences server #2.



- Click **Check IP** to check the IP address. The message “**Success**” (on a green background) should display briefly next to the button.
3. When done, click on **Next** to move to *Integration* tab.

The integration menu displays.

- Check that Integration parameters are properly setup, as part of [2.19 Job Card IST011 - Integration on page 221](#), then click on **Apply**.

### 2.20.3.2.2 Nodes setup

1. From the **Service Tools / Initial Configuration** menu:
  - Click on **Scalability**.
  - The "Manage and display scalability setting" interface will display
2. After a moment, the Nodes table will be populated with the information of the AW Server, as in the example below.

NODE [IP ADDRESS]	CLIENTS	APPLICATIONS	SLICES	CPU	MEMORY	DISK	VERSION	LICENSE SERVER
bucaw71-37 [192.1.1.1]	0	0	0	13%	3022MB / 65536MB (5%)	/dev/sda4 14GB / 41GB (35%) /dev/sda2 1GB / 9GB (12%) /dev/sda1 0GB / 9GB (0%) /dev/sdb1 0GB / 3GB (0%) /dev/sdb2 5GB / 94GB (6%)	Golden set has not been set yet	P: 3.249.70.232 S: Unknown
bucaw71-38 [192.1.1.2]	0	0	0	15%	3063MB / 65536MB (5%)	/dev/sda4 14GB / 41GB (35%) /dev/sda2 0GB / 9GB (0%) /dev/sda1 0GB / 9GB (0%) /dev/sdb1 0GB / 3GB (0%) /dev/sdb2 5GB / 94GB (6%)	Golden set has not been set yet	P: 3.249.70.232 S: Unknown

- Click on **VERSION** information to display the version of the Applications installed.

The Version information may display in red, as the “Golden set” has not been defined yet.

- Use the **Refresh** button to display the other servers of the cluster, if they have already been setup in the cluster mode and are ready for operation.

## NOTICE

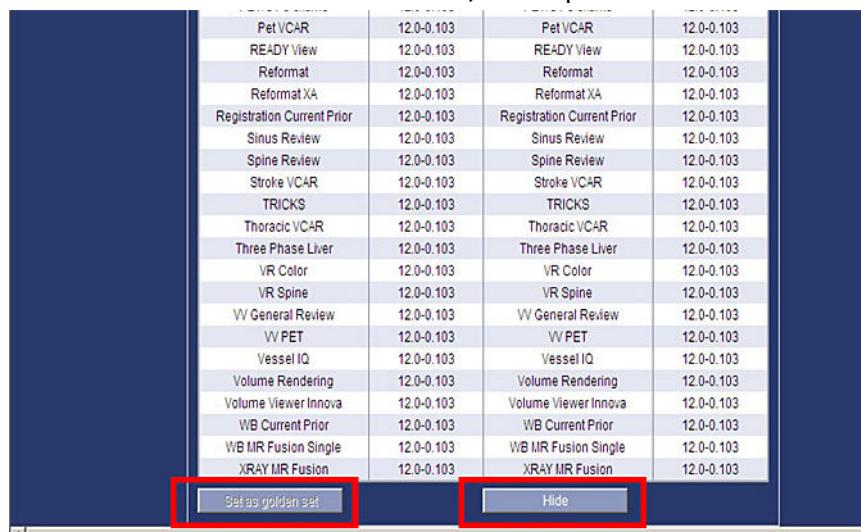
Applications must be installed and activated prior to setting the *Goldenset*. Skip next step if Applications are not yet installed (in which case the *Golden Set* will be done as part of Applications Installation job card). Refer to [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#).

### 2.20.3.2.3 Golden Set setup

#### NOTICE

**To setup the Goldenset, the node MUST NOT be in Maintenance mode.**

- Bypass this step upon initial installation of the system, as you are not allowed to exit the Maintenance mode as long as the Configuration registration key has not been obtained, as a result of sending the Configuration file to the AWCTT web site.
  - Proceed to [2.22 Job Card IST013 - System Configuration Registration on page 259](#) completion, exit the Maintenance mode and return to this step when done.**
  - Click on the **Set as Golden set** button, to setup these versions as the reference versions.



The Goldenset only shows Applications that are active.

- When done, click on **Hide** button to close the window

2. When the Goldenset has been set, the nodes will display **OK** in the **Version** column, as shown in the example below:

		Refresh	Delete selected nodes						
	NODE [IP ADDRESS]	CLIENTS	APPLICATIONS	SLICES	CPU	MEMORY	DISK	VERSION	LICENSE SERVER
	bucaw71-37 [192.1.1.1]	0	0	0	0%	3113MB / 65536MB (5%)	/dev/sda4 14GB / 41GB (35%)  /dev/sda2 1GB / 9GB (12%)  /dev/sda1 0GB / 9GB (0%)  /dev/sdb1 0GB / 3GB (0%)  /dev/sdb2 5GB / 94GB (6%)	OK	P: 3.249.70.232 S: Unknown
	bucaw71-38 [192.1.1.2]	0	0	0	7%	3146MB / 65536MB (5%)	/dev/sda4 14GB / 41GB (35%)  /dev/sda2 0GB / 9GB (0%)  /dev/sda1 0GB / 9GB (0%)  /dev/sdb1 0GB / 3GB (0%)  /dev/sdb2 5GB / 94GB (6%)	OK	P: 3.249.70.232 S: Unknown

#### NOTE

When the Golden has not been set up (version status red), be careful to set it only after all applications have been installed. If the Golden Set has a mismatch (version status red), analyze the cause of the mismatch, identify the correct configuration and make the appropriate changes to the non-compliant server.

3. In our example above, with 2 nodes in the cluster, we can see the following:

- bucaw71-37 is the node we are currently connected on. It is in Maintenance mode (see symbol as in the list below)
  - bucaw71-38 is accessible through a link.
- Clicking on the link will launch the Service Tools web page of those AW servers.
- The Goldenset has been set.
  - The Version and the installed Applications versions are compatible (the same on each server of the cluster, so they display OK).
  - CPU usage, memory usage, Disk usage are OK and do not report a problem.

#### NOTE

Moving the arrow over the NODE IP ADDRESS title field to display the colors and Icon codes table as follows:

NODE [IP ADDRESS]	CLIENTS	APPLICATIONS	SLICES	CPU	MEMORY	DISK
[17] [1.1]						

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:

- 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)

Note: The host name is a link also to the Service Tools page of the node.

4. The HAPS nodes display the IP address and the status of both HAPS nodes. See example hereafter.

<b>Highly Available Preference Storage (HAPS)</b>				
IP address	Free disk space	Total disk space	Preference directory	Available
192.1.1.4	37.6GB	41.2GB	/var/awsprefs	Y
192.1.1.3	37.6GB	41.2GB	/var/awsprefs	Y

#### **NOTE**

When a HAPS node is not available, it just shows the IP address, empty cells for disk space and preference directory and "N" status for the *Available* column.

5. Reboot is necessary for Scalability to be fully operational for the Clients.

You may do it now or proceed with the next configuration steps and wait until the server is fully configured.

- If you want to reboot now, click **Reboot**

#### **NOTICE**

From AW Server 3.2 release, the Users Preferences in Scalability mode are no longer stored on the virtual AW servers, but on two additional redundant HAPS nodes.

The Scalability configuration is complete.

**Proceed to** [2.22 Job Card IST013 - System Configuration Registration](#) on page 259.

## **2.21 Job Card IST006 - Changing the Passwords**

The account 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 passwords.

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

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 requires that the server's system 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. **No system shall be handed over to the customer with the default root password under any circumstances.**

**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.**

**NOTICE**

When changing the passwords DO NOT MISS to notify the OLC representatives. Failing to do so would no longer allow access to your system from the OLC support teams.

**NOTE**

If the Secured for RMF mode is planned to be activated, then perform the password change both for Linux users/accounts and local users only after the RMF mode activation. Refer to [2.31.3.3 Finalizing configuration after Secured for RMF Mode activation on page 461](#) (RMF mode will introduce more strict password policies).

## 2.21.1 Passwords Change Procedure

### 2.21.1.1 Identify New Password(s)

The customer may request specific passwords. If this is the case, get the passwords from the customer and move on to [2.21.1.2 Changing Linux passwords on page 251](#). Make sure that the passwords chosen by the customer comply with the rules listed below.

**NOTE**

For the systems connected via RSvP, the passwords for **root** and **filetransfer** Linux users/accounts, are generated and synchronized with the RSvP server (GE Backoffice), as described in [2.21.1.2 Changing Linux passwords on page 251](#).

If a new password is to be created, the FE should do so in the following ways:

- If required, use customer rules and guidelines for password creation.
- If the FE is free to choose the password, use the following guidelines:
  - Must be 8 to 15 characters min. and 63 characters max.
    - 8 characters min. for AW Server user passwords (default value that can be changed)
    - 15 characters min. for Linux passwords
  - Must contain 1 digit
  - Must contain 1 upper-case letter
  - Must contain 1 lower-case letter
  - Must contain 1 non-alphanumeric character
  - Must not be a palindrome
  - Must not be blank or left as the default
  - Must not be made up solely of dictionary words or easily guess
  - Must not contain 3 consecutive identical characters
  - Must not contain a blank space
  - Must not include your logon name
  - Should not be the same value at different sites

<b>Good password examples:</b>	<b>Bad password examples:</b>
<b>!414585MR5test\$</b>	<b>414555AWS5</b>
<b>4\$42CTAWServ3r32</b>	<b>operator</b>
<b>big996622LS16ct*</b>	<b>123456789a</b>

The following characters (which the system may assign a special meaning) should be avoided:  
`@ ; # ; <Tab> ; <Esc>`; etc .... However, `#` can be used for the `root` password.

#### **NOTICE**

Each account on a single system should have a unique password. For example, the `root` and `admin` accounts should have different password values from each other. Using the same password for multiple accounts on a system will remove role-based access and decrease the level of security on a system.

For productivity, the same password value for a single account can be used on multiple systems at a site or customer. For example, the `root` user/account could have the same non-default password value on 3 different systems in a hospital. However, make sure not to use the same value over multiple sites or across a region, because that would essentially duplicate the original default value problem this service note attempts to resolve. For this reason, procedures are given below for alternative AW platform releases.

### **2.21.1.2 Changing Linux passwords**

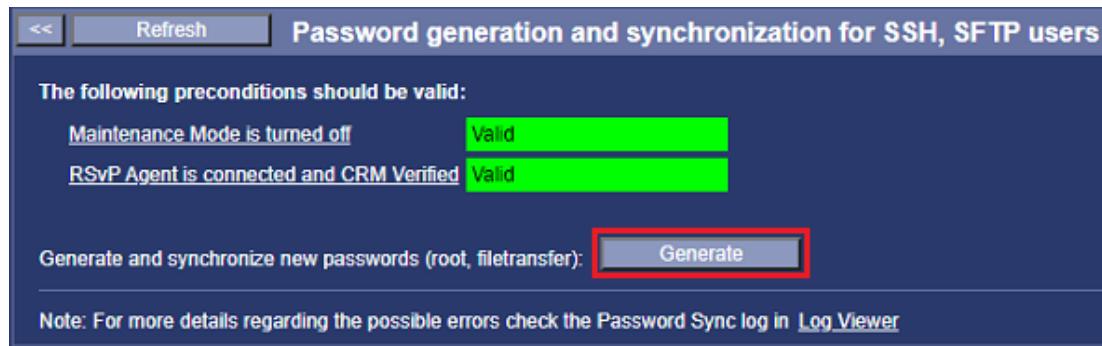
To change the passwords for `root` / `filetransfer` Linux users/accounts follow the below steps:

1. If the system is connected via RSvP, the passwords for `root` and `filetransfer` Linux users/accounts, can be generated and synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault:

#### **NOTE**

In case of a full AW Server installation the Linux passwords can be changed later as the Configuration must be registered prior to turn off the Maintenance Mode

- a. From the Service Tools, select **Administrative > Configuration > Users (OS)**.



- b. The Maintenance Mode must be turned off. If the status is `Invalid`, click on **Maintenance Mode is turned off** to open the *Server maintenance tasks* page. In this page, select **Finish maintenance**.
- c. The RSvP Agent must be connected and CRM Verified. If the status is `Invalid`, click on **RSvP Agent is connected and CRM Verified** to open the RSvP configuration page. Refer to [2.15.2 Remote Service on page 141](#).
- d. Click on the **Generate** button to generate the new passwords for `root` and `filetransfer` Linux users/accounts and synchronize them with the RSvP server (GE Backoffice).

- e. Remotely through FFA, display the *System Password Vault* panel.

#	App Name	Username	Password	Last Updated	Updated By	Actions
1	ea3	service	*****	Feb-17-2021 12:02:58	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
2	sftp	filetransfer	*****	Feb-18-2021 12:10:59	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
3	ssh	root	Uz\$Un3f+ONazneA SiM.UwwiMKi	Feb-18-2021 12:11:10	AGENT	<a href="#">Hide</a> <a href="#">Copy</a> <a href="#">Change Password</a>

- f. Select the **Show** link to view the new password.

#### NOTE

New passwords are generated and synchronized on a weekly basis, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified.

2. If the system is not connected via RSvP, the Linux passwords for **root** can be changed using a command line window:

#### NOTE

For physical AW Server, the password can also be changed either through the KVM or remotely through the iLO service processor.

- a. Open a command window:

- via the **Service Tools > Tools > Terminal**,
- or via the **SSH** connectivity tool or the **Terminal** tool in FFA.

- b. Login as **root**, using the current **root** password.

- c. To change the current password, type:

**passwd <Enter>**

- d. Type the new password and press **<Enter>**.

- e. To confirm the new password, type it again and press **<Enter>**.

- f. Logout and login again to apply the change.

3. It is STRONGLY RECOMMENDED to test the new passwords before turnover to customer, in order to make sure that there was no typo or mix-up with the local keyboard when the password was changed.

- a. Open another command-line window.

- b. Login with each Linux users/accounts and enter the new passwords.

The operating system is configured to lock accounts for a minimum of 15 minutes after five unsuccessful logon attempts within a 15-minute timeframe. The operating system is configured so that the delay between logon prompts following a failed console logon attempt is at least four

seconds. Do not use the **authconfig** tool in the operating system for authentication configuration, it may overwrite the system hardening settings.

**NOTE**

This fail lock mechanism does not apply to the **root** Linux user account.

### 2.21.1.3 Changing AW Server Users Password(s)

**NOTE**

A secure password policy is set for default EA3 local users and the passwords must be changed (if not already changed) during installation: **admin**, **limited**, **standard** and **service** password.

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

After the password is identified, the FE should make the password changes on the device.

There are **Four** default AW Server users accounts, for which the passwords require change:

- **service** (Permanent account)
- **admin** (Removable account)
- **standard** (Removable account)
- **limited** (Removable account)

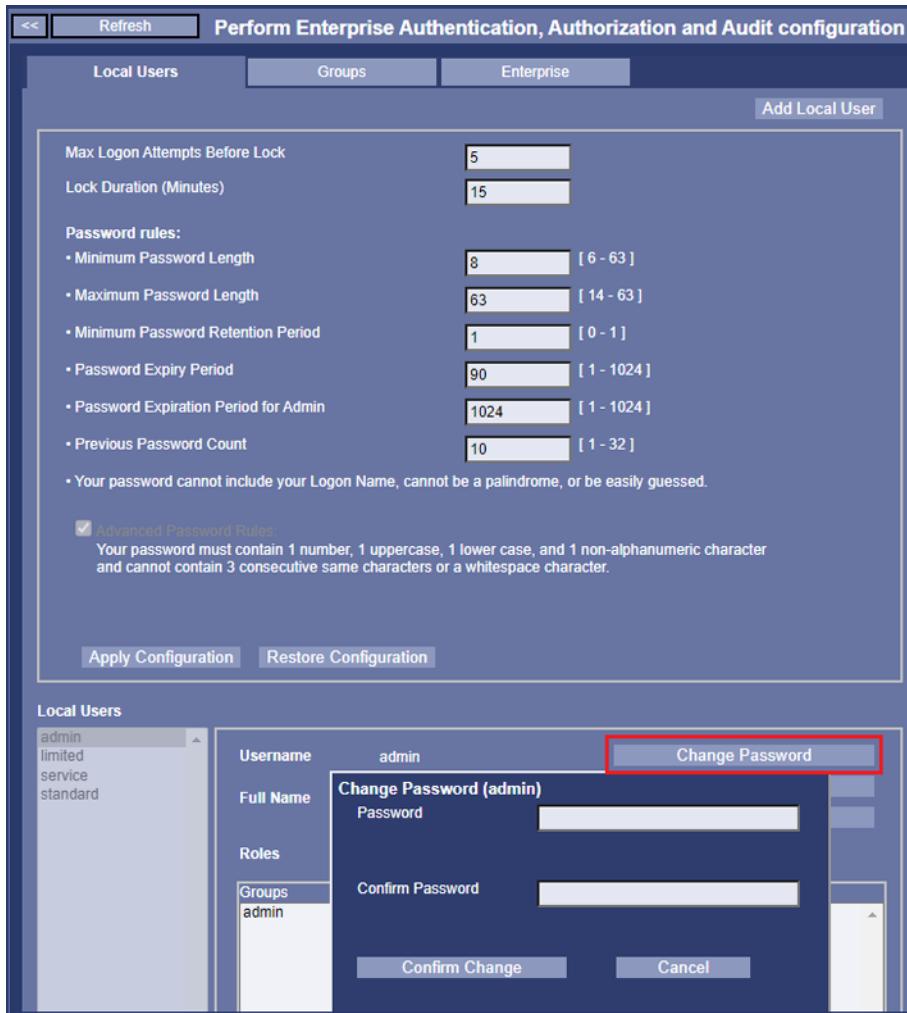
There are two ways to change the AW Server users passwords:

- From the EA3 local users page.
- From the Service Tools login screen.

The AW Server is configured to lock accounts for a minimum of 15 minutes after five unsuccessful logon attempts.

### 2.21.1.3.1 Changing the passwords from the EA3 local users page

- From the Service Tools, select **Administrative > Configuration > Users (EA3)**.



- In the **Local Users** area, select a user account and click on the **Change Password** button.
- In the **Change Password** window enter the new password and confirm it.

#### NOTE

The default password rules can also be changed in this page.

- To confirm the new password, click on **Confirm Change**.
- To change another user's password, repeat the procedure (from Step 2 to Step 4).
- To force the password change at the next login (AW Server Client login), check the **Change Password on Next Login** check box.



#### NOTE

After an upgrade, as the passwords are restored to the default values and/or the password policy may have changed, the password shall be changed. So, check the **Change Password on Next Login** check box.

- Click on **Apply Configuration** button.

### 2.21.1.3.2 Synchronizing the service password with RSvP

If the system is connected via RSvP, the **service** password is synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified:

- 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	Change Password
2	sftp	filetransfer	••••••••	Jun-14-2021 19:07:31	AGENT	Change Password
3	ssh	root	••••••••	Jun-14-2021 19:07:34	AGENT	Change Password

- Select the **Show** link to view the new password.

### 2.21.1.4 Changing Crypto Officer password and Master Encryption Key

On the HPE ProLiant DL360 Gen10 Server, system and data disks are encrypted by default.

If not already done during the server HW installation, the default **Crypto Officer Password** and the **Master Encryption Key** must be changed to customer specific ones in order to increase security.

Refer to the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware), sections “Changing the Crypto Officer Password” and “Changing the Master Encryption Key”.

### 2.21.1.5 Changing the default iLO User name and Password

The procedure is described through the **iLO 5** service processor’s setup menus. It is similar for the iLO 4 and iLO 3 setup procedure.

The HP server’s iLO Service Processor User account shall be factory set and delivered by HP for GEHC to **root**.

The HP servers are also delivered with the iLO user name set to **Administrator**.

It is **required** to change the default **root** account or add a default user and password (in case default user account and password would not have been properly customized for GEHC). **No system shall be handed over to the customer with the default root password under any circumstances.**

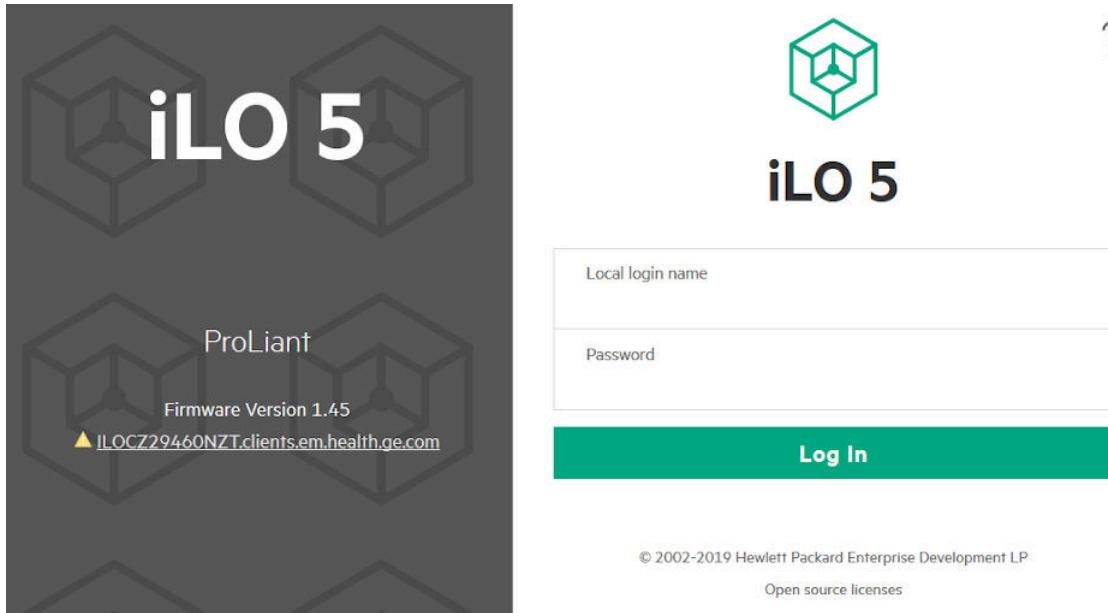
- At the Client PC, or at the FE laptop, open an Internet navigator and connect to the iLO service processor:

`http://<IP_address_iLO-processor>` i.e: `http://3.249.15.122`

#### NOTE

In case you do not have yet access to any of the Client PC, or to the hospital network with your FE laptop, it is possible to use the KVM (keyboard, monitor and mouse) of the server to launch an Internet navigator. Refer to [A.8 Useful Commands and Tools on page 589](#) for details.

2. Login as **root** or as **Administrator** and enter the password written on the paper tag (if applicable):



#### **NOTE**

Use capital **A** for **Administrator** if login as so.

The *Information - iLO Overview* window appears.

3. Go to **Administration > User Administration**.

The *Administration - User Administration* window appears.

Login Name	User Name	Checkmarks
Administrator	Administrator	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
root	root	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

Only the **root** or **Administrator** users should be displayed at this time in the *Local Users* window.

4. To change the **root** password:

#### **NOTE**

For the iLO **root** password, it is recommended to use the same password as the system **root** password to allow remote access to the Server by the Back-Office Team.

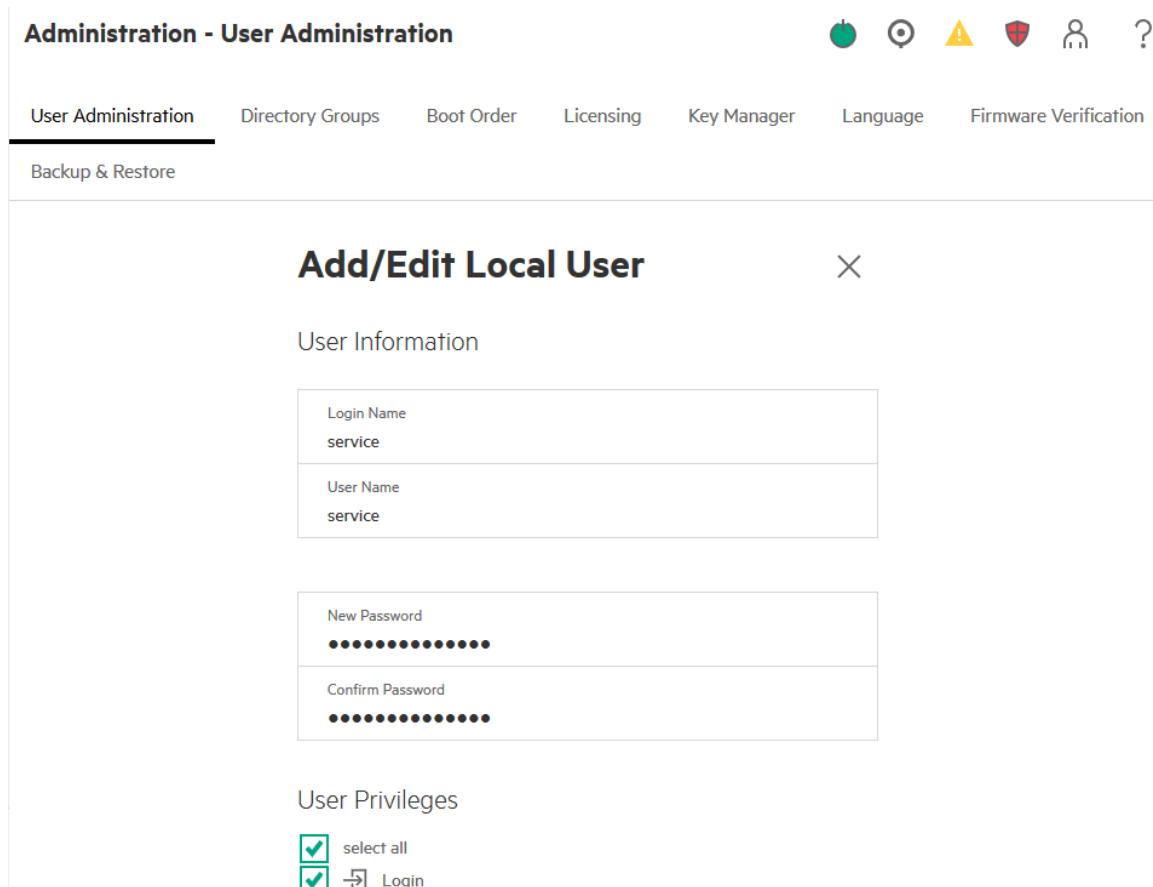
- a. Tick the checkbox next to **root** and click on **Edit**.
- b. Tick the **Change password** checkbox.
- c. Enter the new password twice.

- d. Click on **Update User**.
5. To create a new user, click on the **New** button into the *Local Users* table.

**NOTE**

For the iLO **root** password, it is recommended to use the same password as the system **root** password to allow remote access to the Server by the Back-Office Team.

The *Add/Edit Local User* window appears.



6. Enter the following information:
    - **Login Name.** I.e: **service**.
    - **User Name.** I.e: **service**.
    - **Password.**
    - **Password Confirm.**
  7. In the *User Privileges* panel, tick the **select all** checkbox.
  8. Click on the **Add User** button.
- The new **service** user is created. It allows to login to the iLO service processor.
9. Logout from the iLO Service processor.
  10. Login to the iLO Service processor using the newly created **service** user.
  11. If login to the iLO Service processor using the newly created **service** user is successful, you may delete the original default **root** or **Administrator** user account.
  12. Logout from the iLO Service processor.

## 2.21.2 Updating Password(s) in Connectivity Database

- For the systems connected via RSvP, the password for **root** and **filetransfer** Linux users/accounts and the password for **service** are stored in the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault.
- If the system is not connected via RSvP or for the passwords not available in FFA, update the password in the Connectivity Database and notify the OLC representatives, as described in the table below.

Region	Connectivity Center Information
AMERICAS (US, Canada)	USCAN Connectivity Support toll-free number: 877-842-1132 (8am – 6pm CST, Mon-Fri)
LatAm	<p>Preferably reach the connectivity team via  <a href="https://sc.ge.com/*LATAMcheckout">https://sc.ge.com/*LATAMcheckout</a></p>  <p>or call +55 11 8000 164 702</p>
EU and EMEA	<p>Use the Support Central EMEA Password Change workflow  <a href="https://sc.ge.com/*emeapwc">https://sc.ge.com/*emeapwc</a></p> 
Japan	Call the Connectivity Support number: 0120 596 919
ASEAN	Contact OLE or connectivity champion for re-checkout the system.
ANZ	<p>Call the Connectivity Support numbers Australia 1800 659 465 or New Zealand 0800 659 465</p> <p>OR open a case at <a href="http://sc.ge.com/*ANZConnectivitySupport">http://sc.ge.com/*ANZConnectivitySupport</a></p>
Korea	Call the Connectivity Support (OLE support) number : 1544 6119
China	<p>Call the Connectivity Support number : 400 812 8188</p> <p>OR contact OLE for system checkout/re-checkout</p>
India	Call the Connectivity Support number : 1800 102 7750 (India Call Center) ext 4

## 2.21.3 Communicate New Password(s)

1. Follow your customer's guidelines for password communication and storage. Inform the customer of the new passwords with the exception of those used for remote service only.
2. If the customer approves, write down the new passwords and store them in a secure location on site.  
The [2.21.5 Password Form on page 259](#) includes a sample form to place in a logbook or tape inside a cabinet.
3. In the situation where a customer wants to know more about what GE does with passwords, escalate to the service security team at:

[http://supportcentral.ge.com/products/sup\\_products.asp?prod\\_id=295163](http://supportcentral.ge.com/products/sup_products.asp?prod_id=295163)

## 2.21.4 Performing a system backup

Once you have changed the system passwords, you must perform a new backup of the system as the passwords are part of the configuration that is saved.

### NOTE

In case of a full AW Server installation, the system backup must be done later, in [2.28 Job Card IST016 - System Handover to Customer on page 298](#).

- To perform a system backup, refer to [2.28.2 Backup Parameters and Settings on page 301](#).

## 2.21.5 Password Form



GE Healthcare

Password Change Record for  
System ID \_\_\_\_\_  
By \_\_\_\_\_  
Date \_\_\_\_\_

Login ID	
Password	
Login ID	
Password	
Login ID	
Password	
Login ID	
Password	
Login ID	
Password	

Copyright Pending

The passwords configuration is complete.

**Proceed to [2.14 Job Card IST007 - Service Tools Login on page 131](#).**

## 2.22 Job Card IST013 - System Configuration Registration

Proceed with the following sections to register your AW Configuration and obtain in return the Registration key allowing you to exit from the Maintenance mode, when all the installation and configuration tasks are completed.

**NOTE**

If the Secured for RMF mode is planned to be activated, then do the configuration registration only after successful RMF activation to ensure that AW Server is registered with correct RMF information. Refer to [2.31.3.3 Finalizing configuration after Secured for RMF Mode activation on page 461](#).

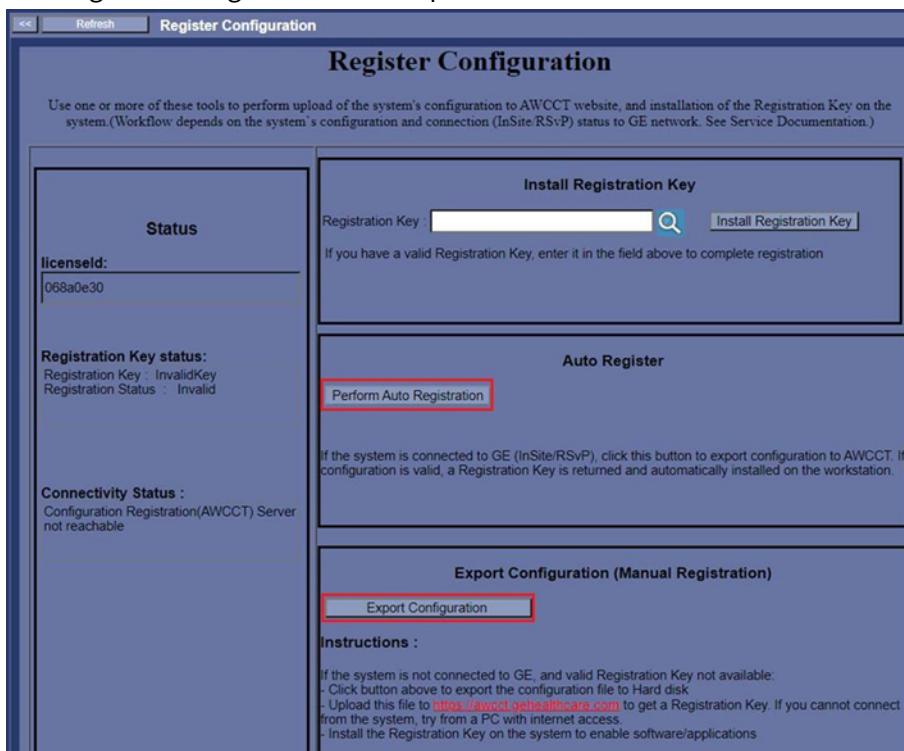
## 2.22.1 Configuration registration steps

- Under Service Tools / **Maintenance** menu, click on the **Register Configuration** link to launch the Configuration Registration tool.

**NOTICE**

*Device Data in Initial configuration* must be configured. Otherwise the Register Configuration menu will not open.

The Register Configuration menu opens.



- CASE 1: If your AW Server is connected via **RSvP** and that the System ID (CRM Number) is verified, you can use the "Auto Registration" process.

Click on the **Perform Auto Registration** button, to automatically send the Site configuration file to the **AWCCT** Web site.

If the configuration is compliant, messages will say so in the Connectivity Status and Registration Status windows and you will automatically receive in return within a few seconds the Registration key, while the "Request in progress" message will change to "*Operation success ! The registration key has been successfully installed*".

- System Configuration Registration is complete. The Registration status field in the HealthPage should display as Standard in green.

Bypass the next steps. They are dedicated to manual registration when remote connection via **RSvP** is not available.

**You are now able to exit the Maintenance mode when desired.**

**AW Servers in Cluster mode** - You are now able to configure the Golden Set.

Refer to [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

- CASE 2: If your AW Server is NOT connected via **RSvP**, you are NOT able to use the "Auto Registration" process. Use the "Download configuration (Manual Registration)" process.

Click on the **Export configuration** button to export the configuration file (in the form *licenseID\_systemID\_date\_Configuration.txt*) to your PC or to a media (e.g. USB stick).

**Nothing may seem to happen for a short moment. Do not click again on Export configuration.**

Select to save the *LicenseID\_systemID\_date\_Configuration.txt* file.

#### NOTE

For physical AW Server, if using the KVM or remotely through the iLO service processor, the configuration file can be found in the */root/Downloads* directory and copied to an USB media. From Firefox, you can also display the downloads and drag and drop the configuration file into the USB media (which is displayed on the desktop once inserted).

- Launch an Internet Navigator and connect to <https://awcct.gehealthcare.com>.

If you cannot properly reach or display the site, right click on the Internet Navigator icon and select "Start in Private Browsing" that will open a new Navigator window.

#### NOTE

If you cannot connect from the AW Server, try from a PC with Internet access.

#### NOTICE

Currently, only the Windows TM Internet Explorer navigator is supported.

- The following AW Configuration Collection Tool screen displays.



Click on the **Browse** button of the AW Service Tools Register Configuration page, then select your AW Server's Configuration file.

Click on the **Submit** button.

- The AW Configuration Collection Tool screen displays the Summary of uploaded Configurations.

If the configuration is compliant, you will get your system Registration key.

The screenshot shows the GE AWCCT web interface. At the top, there's a navigation bar with icons for Home, Documentation, Contact Admin, Advanced Key Management, User Configuration, Off-line Tool License, and Logout. Below the navigation bar, a message says "Hi Philippe Vessieres(100000530), you have logged in with Privileged permission" and "It is recommended to view". The main content area has a yellow header bar that says "Summary of Uploaded Configurations". Below it is a table with one row. The table columns are: File Name, File Upload Status, Registration Key, System ID, and License ID. The row data is: "06bf0e97\_AWBULCLAB\_100000530\_AWS\_20141223101532.txt", "Success", "b44m9zf8b82", "AWBULCLAB", and "06bf0e97". At the bottom of the table, there are two buttons: "Save Registration Key" (highlighted with a red box) and "Click here to proceed with another upload".

Click on **Save registration Key** button, and choose the location where to save the key on your AW Server (if applicable) or on your PC.

#### **NOTE**

For more information about the Configuration Registration tool, refer to the AWCCT User Guide available on AWCCT web site in *Documentation* section (Part number: **5589257-1EN**)

8. Copy/paste or type in the Registration Key in the Install Registration Key field and click on the Register button.

The "Request in progress" message displays, followed by "Operation success" message.

#### **NOTE**

In certain situations, the upload of the Registration key on the AW Server may result in "not configured".

To avoid this, just copy/paste or type in the Registration Key in the Install Registration Key field and click on the **Install Registration Key** Button

9. System Configuration Registration is complete. The Registration status field in the HealthPage should display as Standard in green.

#### **NOTE**

If download of the Configuration file does not succeed, it is possible to send it by email to the AWCTAdmin@ge.com address. You will receive in return by email the Registration key.

**You are now able to exit the Maintenance mode when desired.**

**AW Servers in Cluster mode** - You are now able to configure the Golden Set. Refer to [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

## 2.22.2 Process in case of issue at Registration time

### 2.22.2.1 In case of issue to access the AWCCT Website.

Please follow the rules below:

#### **Context:**

- The AWCCT web site is down
- No SSO available (No GEHC personal - i.e: Distributor)

**Action:** use registration process via email process

- Save AW Server Configuration to hardware or USB media.
- Send it by mail to [AWCCTAdmin@ge.com](mailto:AWCCTAdmin@ge.com)

Registration key and Configuration Registration Report will be returned by mail within 1 hour.

## 2.22.2.2 In case of issue to get the registration key or to install it

In case of issue to get the registration key for your AW Server at installation time or to install it, please follow the rules below in order to get assistance:

### Context:

- AW Server Configuration file not recognized on AWCCT
- Process via email at [AWCCTAdmin@ge.com](mailto:AWCCTAdmin@ge.com) did not return timely.
- Configuration uploaded fine, but returns with non-valid key, or no key returned
- Issue at Registration key installation on AW Server

### Action:

- Contact the Service L3 (RTE/OLE/RSE) team with the following:
  - AW Server's License ID (minimum)
  - AW Server's configuration file (preferably)
- To close the Service case, the Configuration File will have to be uploaded on AWCCT web site as soon as possible.

### NOTE

For any question about the Configuration Registration process, FE can call the Configuration Registration Call Center number at:

**(+1) 855-741-3136** (toll free number from US only)

**(+1) 262-524-5660** (if the first phone number does not work)

Call center support will be done in English language only

The Service Tools configuration is complete.

Proceed to [2.24 Job Card IST014A - Standard Client PC installation & Tests on page 270](#) OR

Proceed to [2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282](#)

Or proceed to [2.26 Job Card IST014C - Web Client Tests on page 286](#).

## 2.23 Job Card IST014 - Server Installation Validation Tests

To validate the AW Server system installation, two tests on the AW Server are required:

- A HealthPage test
- A server diagnostic test

It determines whether the server is working properly, independently of the rest of the system (without the network and client).

### NOTE

This is a test of functionality, not relative performance. Noticeable "hangs" or delays (beyond a reasonable time) might indicate a test failure.

## 2.23.1 HealthPage Test

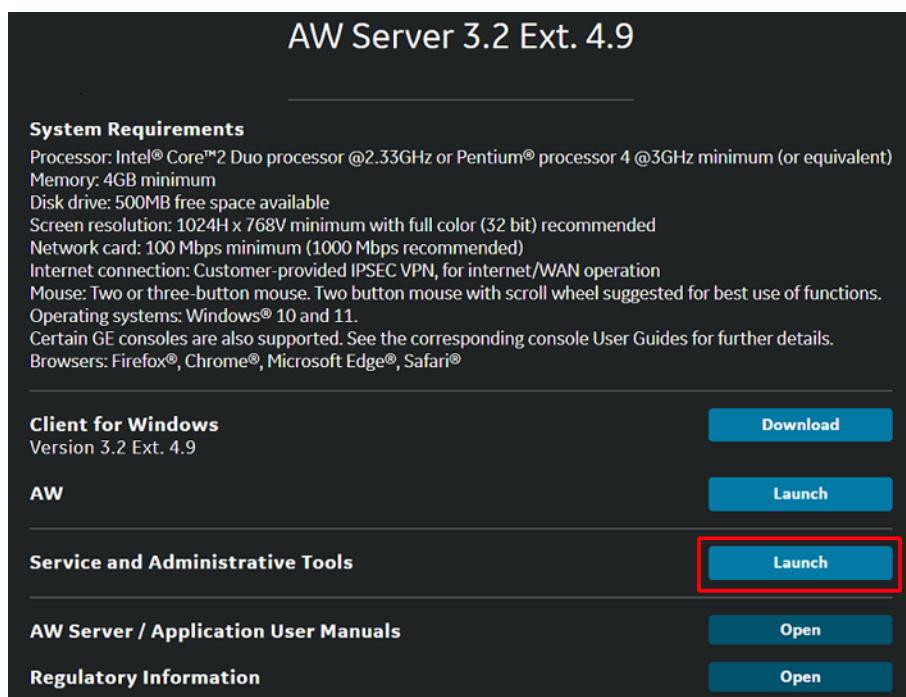
This is the first part of the AW Server Test. The HealthPage evaluates the system hardware and platform software sub-systems.

### 2.23.1.1 Required Tools

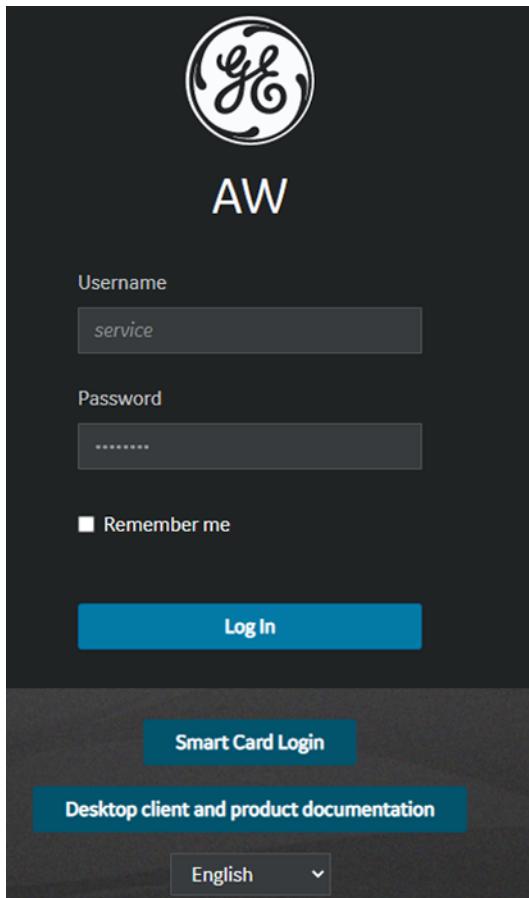
This test requires to connect from the PC on which AW Server client software is installed.

### 2.23.1.2 Procedure

1. At the Client PC, open a web browser and type in:  
[https://<AW\\_server\\_IP\\_address>/](https://<AW_server_IP_address>/)
2. If not already done, accept the cookies in the window that popups.
3. In the landing page, click on *Service and Administrative Tools* **Launch** button.



4. The login screen appears.



5. Login as **service**.

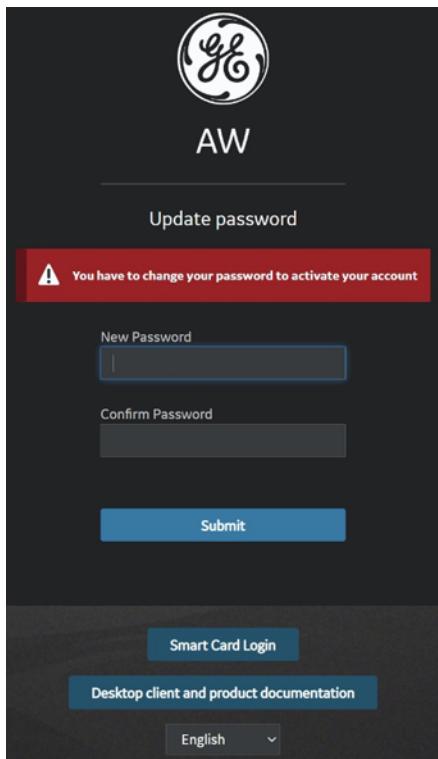
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

**NOTICE**

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for the password change guidelines.

6. The Service Tools HealthPage appears as shown in the following illustration examples.

Hardware Subsystem	Status
Temperature	OK
Fan Status	OK
Voltage	Not applicable
Power Status	OK
UPS Status	OK
RAID Status	OK

For HP servers (High Tier or Low Tier), some fields can display in yellow color when they are OK.

Each right-hand column on this page shows color-coded status information indicated by a GREEN, YELLOW or RED background.

System Configuration	
System ID (CRM Number)	Test123456
Platform version	aws-3.2-4.9-2231.4-01f2d556
Hostname / IP Address	plt101f / eth0: 10.97.225.101
Encrypted (TLS) AET / Port	plt101f / 2762
Plain AET / Port	plt101f / N/A
CPU (12)	Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz
Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9
Modality OS Version	AWS3.2_OS_7.1-2228.5-e5890961 [20220715]
UDI	(01)00840682102384(10)AWS03D02E4D9
REF	5719780
LOT	AWS03D02E4D9
Uptime	4:57
Region / Timezone	Europe / Budapest
Memory Total / Free	24576 (MB) / 19364 (MB)
OS Disk Space Total / Free	361 (GB) / 325 (GB)
Image Disk Space Total / Free	913 (GB) / 714 (GB)
Backup Disk Space Total / Free	3 (GB) / 3 (GB)
Log Disk Space Total / Free	19 (GB) / 18 (GB)
AWeDIM Disk Space Total / Free	68 (GB) / 28 (GB)
Network Queue Status	In progress: 0 Pending: 0 Paused: 0 Failed: 0
Auto Delete (High / Low)	-
Delete option for worklist browser	Off
Image partition mount count (Current / Max.)	1/30
Signer certificate expiration date	Wed 02 Aug 2028 04:19:16 PM CEST
Certificate expiration date	Wed 06 Sep 2023 04:19:17 PM CEST
EC certificates expiration date	N/A
Clam AV Antivirus Software status	Not activated
Machine type	ProLiant ML350p Gen8
Install mode	server
DICOM AET (printing)	PR_plt101f
Service Processor	3.249.65.180
License ID	8b58088e
Integration	Full front end integration (Hybrid)
Cluster mode	False
Registration status	Permanent
Registration key	69bbdz826ed
Automatic Configuration Status Summary	N/A
Secured for RMF	Off
RMF activation date	N/A
RMF verification date	N/A
Hardening status	Off
Hardening activation date	N/A
Hardening verification date	N/A

- Green means that the status or value of that item is OK.
- Yellow means not critical (i.e: Mount count for fsck is highlighted in Yellow if the values are close to max values)
- Red indicates a problem. Any item with a red background indicates a failure which must be investigated and fixed.
- A white background indicates that “status” is not applicable for that item.
- Not applicable for the image partition fields means that the system is integrated to the PACS and does not manage the image database.

7. Check the *Hardware Subsystem* area:

- a. Click on the **Sensor Details** button (GEHC delivered hardware) to display all available hardware sensor data. Verify that there are no problems.
- b. Or click on the **Status Details** button (virtual AW Server) to display the virtual hardware resources. Verify that there are no problems.

**GEHC delivered hardware:**

- 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 standalone 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.

**Virtual Machine:**

- A RED indicator in the Hardware Subsystem for Virtual Machine status may mean incorrect hardware resources: Contact IT admin of the hospital to update the virtual resources provided to the Virtual Machine.

8. Check the *System Configuration* area:

- a. Check the basic server parameters. The previous illustration shows normal values for the AW Server as of this writing.
- b. Hover your mouse cursor over each green or red item in System Configuration to see additional information.

9. Check the *Software Subsystem* area.

This area 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.

**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.

10. Check the *Software Subsystems essential for Service Tools* area.

- This area shows the status of services which must be running in order for Service Tools to work.
- A RED indicator in the Software Subsystems Status table indicates a failure in the server software subsystem.

**NOTE**

Some of these failures (e.g., filer 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 is also 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 by clicking on **Restart**

#### **NOTICE**

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 command line:

```
/usr/share/ServiceTools/scripts/healthpage/restart_st.sh  
/usr/share/ServiceTools/scripts/healthpage/restart_all.sh
```

(the **Restart** button is mapped to this script)

- Reboot of the server – disconnects 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 standalone test has passed.

## 2.23.2 Server Diagnostic Test

The second stage of the AW Server 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.

The screenshot shows a window titled "Perform server test". At the top, there are buttons for "Refresh" and "Perform server test". Below the title, there 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 table 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 Standalone Diagnostic has passed, and the server is now ready for system/client testing.

This concludes the AW Server standalone test. The procedure in the next section will test the entire AW Server system – the server, the client, and the network.

## 2.24 Job Card IST014A - Standard Client PC installation & Tests

This Job Card applies to the installation of Clients for Standalone (Non-Integrated) AW Server or for all integrated AW Server other than the Seamless integration.

**For installation of Clients in Seamless integration, please refer to:**

[2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282](#)

**Foreword****Windows Client:**

The GEHC FE is responsible for installing at one Client PC and to discuss with the IT administrator that all other client PCs must be installed as well. It is normally the responsibility of Customer to install all the rest of their existing client PCs. Provide the Clients installation procedure to the IT Admin.

**Windows Client - Mass Installation:**

It is under the Hospital responsibility to install all other Client PCs. If the hospital decides to use the Microsoft MSI mass deployment software, they will do it under their responsibility.

The MSI package is available in the AW Server SW & Docs Set.

### 2.24.1 Client Installation Procedure

#### 2.24.1.1 Windows TM Client PC installation Procedure

##### 2.24.1.1 System Requirements

The minimum hardware and software requirements for the client are listed on the AW Server main page, as shown in the following illustration of the AW Server main screen.

**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 and 11.  
Certain GE consoles are also supported. See the corresponding console User Guides for further details.  
Browsers: Firefox®, Chrome®, Microsoft Edge®, Safari®

**Client for Windows** [Download](#)  
Version 3.2 Ext. 4.9

**AW** [Launch](#)

**Service and Administrative Tools** [Launch](#)

## NOTICE

DO NOT install client software on more than one client PC per customer! NO EXCEPTIONS!

The GEHC customer contract specifies that GEHC will install AW Server software on only ONE client, for the purposes of testing the AW Server system upon installation. If a GEHC FE installs and/or configures the software on more than one client per customer, IT CAN CREATE SERIOUS LEGAL AND REGULATORY PROBLEMS FOR GEHC. Except for the first client (which is set up by the GEHC FE), THE CUSTOMER MUST INSTALL AND CONFIGURE THEIR OWN CLIENTS.

### 2.24.1.1.2 Installation requirements

#### NOTICE

You need administrative permissions on the client PC to download and/or install the AW Server client software. If you don't have it, ask the site IT Admin to change the permissions temporarily, or have the IT Admin install the client software as the Admin user. Make sure you have current contact information for the site's IT administrator, in case you need his/ her help during this procedure.

### 2.24.1.1.3 Client Installation Errors/Problems

It is not possible to anticipate ALL potential site security, filters, and firewall rules for this product. Make a note of any errors in the client installation process, because they might be related to PC and/or network security / firewall configuration.

Client problems are the responsibility of the customer!

#### NOTE

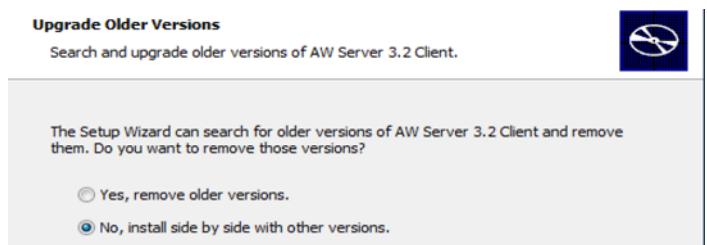
The AW Server Client program must be downloaded and installed on the client PC to use the AW Server as a product. If you are unable to do this, ask the site IT Admin to help you find the reason.

### 2.24.1.1.4 Downloading the AW Server Client Software installer

- On the PC that will be used as the client, launch a web browser (refer to [1.6 Supported Web Browsers on page 27](#)).

**NOTE**

Different AW Server Client releases can reside on a Client PC (e.g. your site has an AW Server 2.0 that is in use and must be kept operating, and has purchased a new AW Server 3.2). To uninstall an older AWS Client, you can select the option “**Yes, remove older versions**”. If the shortcut remains on the desktop, delete it manually.



**NOTE**

In certain cases, you may also need to remove an older Client, prior to installing the new one. In those cases, first remove the older client on your Windows TM PC using: **Control Panel > Programs > Programs and Feature > Uninstall or change a program** to uninstall the older Client.

- Enter the AW Server’s IP address (for example, <http://3.70.211.201>) into the browser’s address bar, then press **<Enter>**.

The AW Server main page displays a page similar to the example shown below:

**AW Server 3.2 Ext. 4.9**

---

**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 and 11.  
Certain GE consoles are also supported. See the corresponding console User Guides for further details.  
Browsers: Firefox®, Chrome®, Microsoft Edge®, Safari®

---

**Client for Windows**  
Version 3.2 Ext. 4.9

**Download**

- Click the **Download** button next to Client for Windows to download the installer file for the AW Server client.
- When the client installer file has downloaded completely, save it to the desktop.

### 2.24.1.1.5 Installing the AW Server Client

- When the installer file has downloaded completely and is saved on your desktop, double-click the corresponding icon to run it.
- If a security warning such as “publisher of the setup software could not be verified” displays, click on **Run**. (The exact wording of the warning will depend on which browser you are using).
- The Windows setup wizard interface will display. Click **Next**.
- The *Select Installation Folder* interface will display. Keep the default path (e.g. C:\Program Files\GE\AWS\_3.2) or use the **Browse** button to select a custom path.
- Click **Next** when done.

**NOTICE**

When "remove older version" message is display, and when accepting removal, pay attention that it will remove all major versions as well (AWS2.0, AWS3.1). When updating AWS3.2 on existing AWS3.2 version, a manual uninstall may be necessary first.

5. • The *Ready to install* interface will display. Click **Install**
6. • The *Completing the Setup Wizard* interface will display. Click **Finish**.
7. • Verify that the new AW Server client program is listed in the Windows **Start** Menu.

**The AW Server Client software is now installed on this client PC**

**NOTE**

If the site is running a Chinese, Japanese or Korean UI in a Windows 64 environment, you must change the Language and Regional settings on the Client PC.

- 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".
  
- 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".

**8. AWS Client configuration for CPACS integration**

- In case of hybrid integration between AWS and CPACS, it is necessary to modify the AWS Client files. This is needed because CPACS might be blocking specific processes like solo.exe. Refer to section [2.24.2.5 AWS Client configuration for CPACS integration on page 281](#) for detailed procedure.

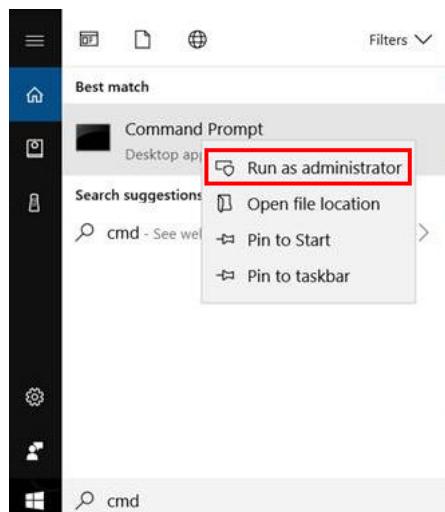
**9. AWS Client configuration for upgrade from AW Server 2.0**

- To enable the Close button on the User Interface (instead of the usual Logout button that can be seen in the Standalone (No-integration) mode), you need to modify the solo.ini file. Refer to section [2.24.2.6 AWS Client configuration for upgrade from AW Server 2.0 on page 282](#) for detailed procedure.

**10. Silent install**

When launching the AW Server Client for the first time, the user has to manually enter the IP address(es) of the AW Sever(s) he/she wants to reach. And that for every AW Server Client. To avoid this waste of time, the AW Server Client can be installed in "**Silent**" mode from a **Command Prompt** using the Windows installer as follow:

- When the installer file has downloaded completely and is saved on your desktop.
- Open a **Command Prompt** as administrator.



- In the **Command Prompt** enter the following command:

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

<user>: Is your Windows username

**IPLIST:** Contains the list of the IP addresses of the AW Servers you should be able to reach. Here as an example there are 2 IP addresses corresponding to 2 AW Servers.

#### NOTE

The IP address can be replaced by the hostname if the hospital uses a Domain Name system.

**install.log:** After the installation process, the install.log file will be created in the specified folder (here \tmp), which contains information about valid or invalid IPLIST items.

#### NOTE

The command returns immediately but works in the background for several seconds.

- Finish the installation with step 7) above.

#### NOTE

The AW Server Client installation in "**Silent**" mode is not available for Seamless integration

## 2.24.2 Client (System) Test

The final validation test of the server installation tests the AW Server as a system by connecting to a client PC via the site's network. This includes a basic test of the client itself

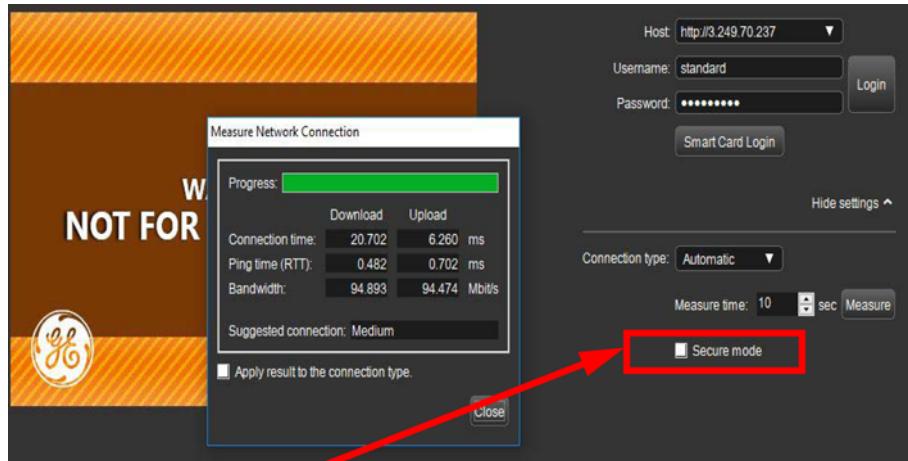
- 1.) • On the client PC, start AW Server by double-clicking on the AW Server icon on the desktop. The AW Server Splash Screen should display briefly, followed by the AW Server Login screen after a few moments.



### NOTICE

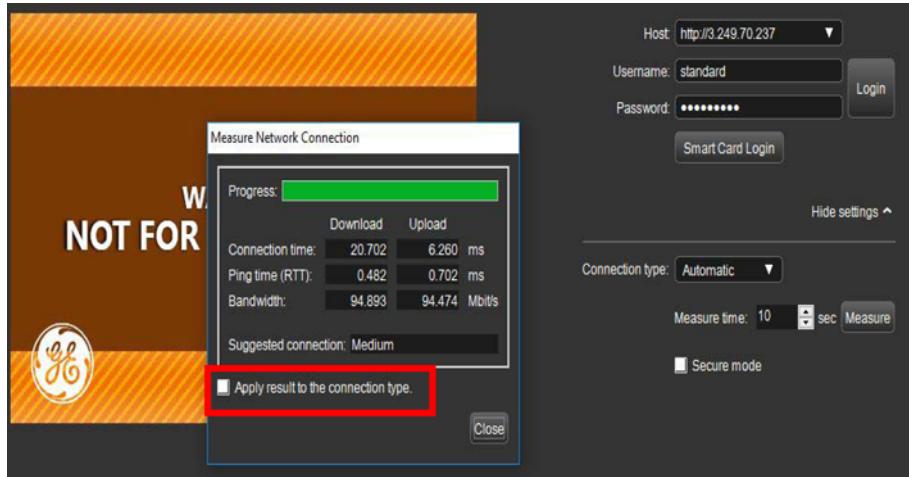
If a banner like in our example pops up displaying the message "Not For Clinical Use", it means that the release installed is not a supported release.FE should warn the customer that upgrade shall be done immediately, as the installed release is not validated/supported.

- 2.) • Click on the **Show settings** link to show/hide additional connection information.



- 3.) • **Optional:** If necessary, see the AW Server Service Manual for information about the Extra Security Layer, click on the "Secure Mode" check box. Basically, you shouldn't need this when connecting from the site's internal network.
- 4.) 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

- 5.) When the Network Connection measurement has completed, you will get the following result window.



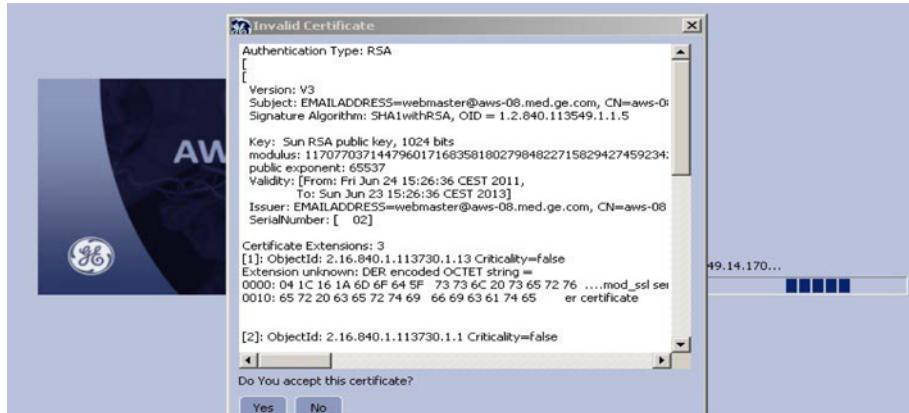
The suggested Connection type will also be displayed.

- You can click on **Apply results to the connection type** check-box, then click on the **Close** button to apply the suggested connection type to your Client PC.
- 6.) Now you can login to the AWS Client.
- Enter a valid local server account name and password (e.g., service), or a valid enterprise account name and password. If the enterprise account server configuration is complete, see the Enterprise Accounts Configuration section of this document.

#### NOTE

If you have selected the secure mode, and that the account is valid and the server is reachable, the AWS client will login to the AW Server. An "Invalid Certificate" window will pop-up at first login (as shown in the following illustration) if the site has not purchased an authentication certificate controlled by a third party. This "Invalid Certificate" window means that the AW Server is using a self-signed certificate. If the customer does not want to use self-signed certificate, he/she will have to purchase a certificate validated by a CA on its own.

- 7.) The Certificate window pops up.



- Click **YES** to accept.

### 2.24.2.1 Network Test (summary and client information)

This test displays client bandwidth information for up to ten recent tests.

If the PC can access network resources, and download the AW Server Application, it is network functional for AW Server purposes.

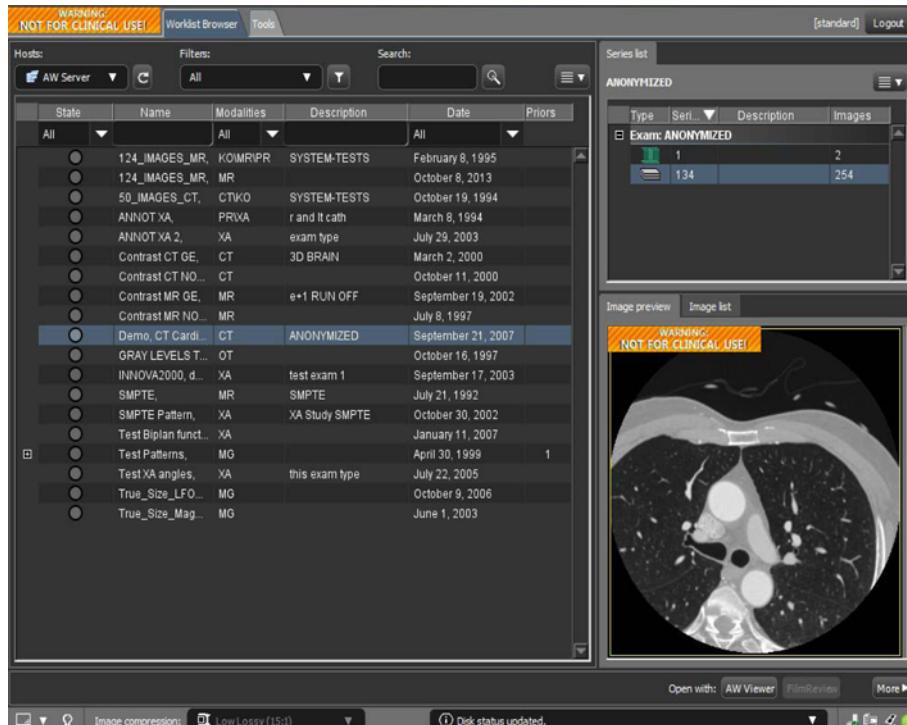
## NOTICE

This tool evaluates the client configuration and monitor to determine if they meet the basic requirements for the AW Server client application. This check is only an initial evaluation of the operating system and hardware specifications. It is NOT meant to replace normal QA procedures.

### Client Worklist Browser Test

This procedure is a basic “launch-and-go test” to validate basic server operation.

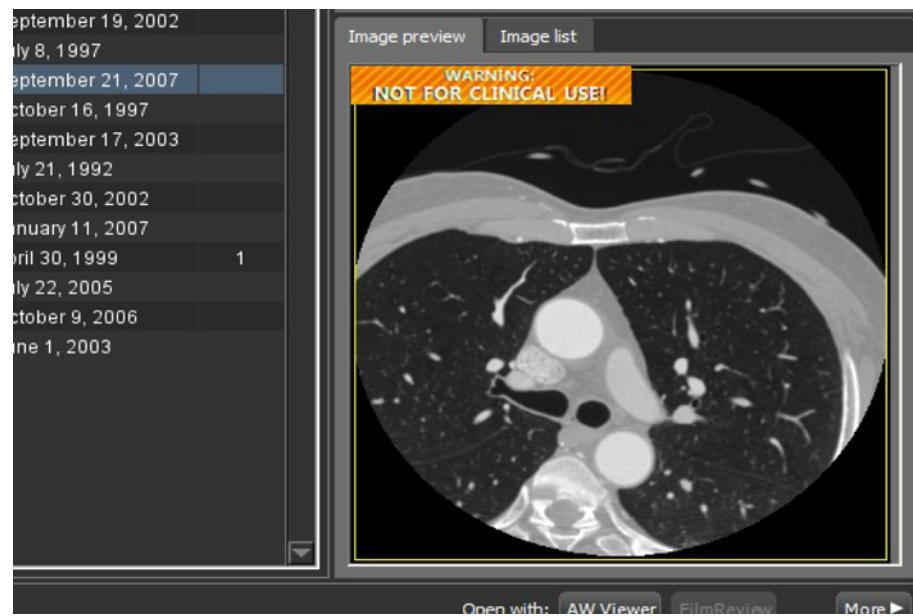
- 1.) Launch the AW Server Client Worklist Browser. It should display as shown in the following illustration example..



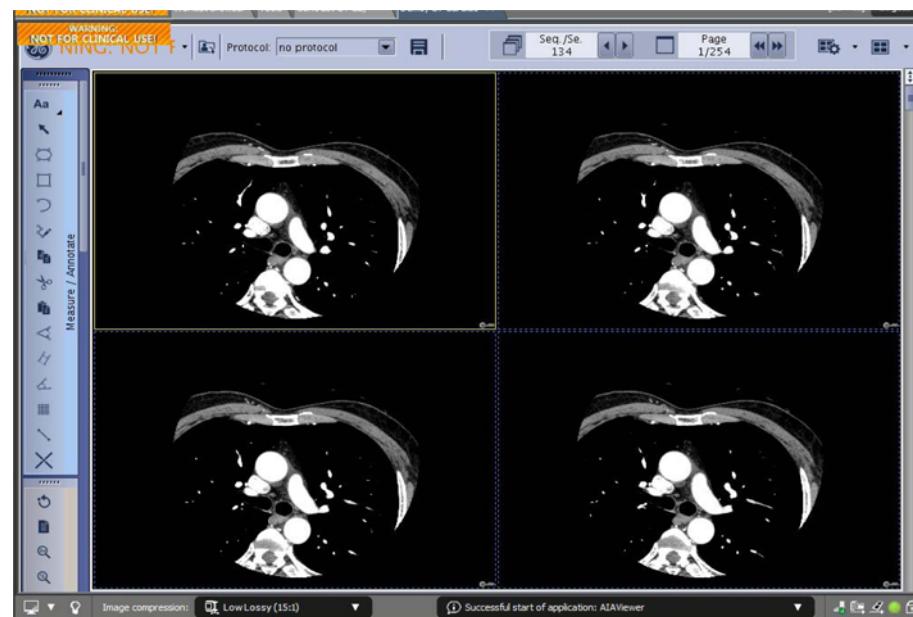
- 2.) The browser displays exam datasets, advanced applications launch buttons (when applicable), and remote DICOM host queries, among many other functions.
  - Select an exam from the list of exams in the browser.

You must have an exam source (a PACS, etc.) configured before any exams will be listed. For detailed information on this tool, see the User Guide Document from the AW Server UI.

- 3.) • Select a series image-set in the Series List. The Image preview window (at lower right should display an image from the selected series, similar to the example shown:



- 4.) • From the "Open with" menu, click **2D Viewer**. The 2D Viewer application should launch with images in the right two-thirds of the frame, and tools in the left third as shown:



- 5.) • Experiment briefly with some of the tools and controls and verify that they respond as expected. (See the User Manual for details.)
- 6.) • Click on the tab (at the upper left) "X" to close the 2D Viewer. The display should go back to the exam list and series image display.

- 7.) • Click the 3D Viewer button near the bottom right of the screen. The Volume Viewer launch splash screen should display, then the protocol selection and tool frame should come up as shown in the following illustration.



- 8.) • Click on one of the protocols (for example, “**Reformat**”). Verify that the screen displays and changes as selected.
- 9.) • Close the 3D Viewer tab.
- 10.) • Click the **Worklist** Browser tab in the upper left corner of the browser. The original browser patient list should display again.
- 11.) • Exit the browser, either by clicking the Logout button at upper right, or by clicking on the upper right corner “X”.

This completes the basic operational validation test. If all steps passed successfully, the AW Server system is operating correctly.

### **NOTICE**

If any of the preceding steps produced error messages or made the display hang or display artifacts, this system validation test has failed, and the AW Server is NOT ready for customer use. Read the “Validation Test Failure – What to do” and “Troubleshooting Tips” in the following paragraphs.

## **2.24.2.2 Validation Test Failure – What to do**

In the event of system validation test failure:

- Examine error(s) and corresponding error logs using the Log Viewer in Service Tools.
- Re-run the StandAlone diagnostic process.
  - If it passes, there could be network-related or client-related issues.
  - If it fails, pursue the suggestions in the standalone diagnostic section of the AW Server Service Manual.

Other suggestions in the event of system validation failure:

- Remove and then re-install the advanced application(s) package(s) using the Version Management tool in Service Tools. (Reference the Service Tools section of the AW Server Service Manual.)
- Reload both the OS and platform software (Load From Cold).

### **Validation Test Troubleshooting Tips**

If you cannot perform the “Installation Validation Tests” successfully, troubleshoot the component that is failing. See examples below:

- If you cannot connect to the server web page, troubleshoot connectivity-related issues:
  - Can the PC access other resources on the local network (LAN)?
  - Can the PC access the Internet?
  - Is the PC configured correctly on the network with a valid IP address, netmask/network prefix, and gateway?
  - Is there an Internet proxy configured in the browser?
  - Does this PC require a proxy to be configured?
- Remember, a proxy allows an internal network PC a gateway to an external network (like the Internet). If the browser attempts to use this proxy to access an internal network resource – like the AW Server – it will not be able to find it. Conversely, if the PC needs a proxy to get from the network it is on, to a remote network (like the Internet), and there is no proxy configured, the PC will not be able to connect.
- Proxy configurations should be discussed with the site IT admin. For test purposes, they can be turned off or on to see what the effects are. BUT, doing so could result in other network resources becoming non-functional until the proxy settings are returned to normal.
- Use “ping” and “traceroute” to test and verify the network functionality. The Service Tools --> Diagnostic --> Test --> Network tool does some of this for you.
- Try to narrow the connectivity issue down to either a CLIENT issue or a NETWORK issue. A good way to do this is to test multiple clients on the same subnet. If they all act the same on the same subnet, chances are there is a network issue. If only one has the problem, focus on it.
- IT IS ALSO VERY HELPFUL TO PERFORM A SIDE-BY-SIDE TEST USING A DUAL-CORE PC, SUCH AS A GEHC SERVICE/SALES LAPTOP. This is especially useful for “performance” issues, to determine whether or not the client PC is the problem, and to validate the server.
- Remember, the NETWORK and the CLIENT (other than installing AW Server client software on ONE customer client as specified in the contract) are NOT the responsibility of GEHC. Once the server is proved to be working correctly, and that the problem resides with the network or the client, the AW Server service model is validated, and the final resolutions for issues related to the network or client belong to the customer.

### This completes the AW Server Installation process.

Once the system passes these validation tests, it is ready to be turned over to the customer for applications training and/or normal use. This is described in the next Job Card.

#### **NOTICE**

Please remember to log only actual installation time against the server’s installation dispatch. Use TRAINING (or another appropriate account) to log ‘observation’ or ‘non-installation’ site AW Server activities. Also make sure to include in the installation dispatch the “completion” comments: "HW verification complete prior to software install"

## **2.24.2.3 Printing tests**

### **2.24.2.3.1 DICOM printer(s) tests**

If you have installed one or several DICOM printers, make sure they are correctly setup by printing some demo images under AW application.

### 2.24.2.3.2 Printing with a site's Postscript printer

On a Client's Windows PC, if requested by the customer, it is possible to use the declared Postscript printer(s) together with the AW Server application, by pressing simultaneously on the <Ctrl> <P> keys.

However, this may not be directly achievable, depending on the version of the Postscript printer's drivers.

If Postscript printing does not work, here are the recommendations to forward to the IT administrator:

- Retrieve the latest drivers for the printer from the Internet
- Manually declare the printer on the PC from Start/Settings/Control panel/Printers & Faxes, using the downloaded drivers.

### 2.24.2.4 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.

#### **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.
- 

#### **Procedure for Windows Client PC running Windows**

Use the Windows Explorer to edit the "solo.ini" file.. Go to **C:\Program Files (x86)\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
<b>2MP monitors</b> (1920x1200)-	DmaxNXWidth=1920 DmaxNXHeight=1200
<b>3MP monitors</b> (2048x1536)	DmaxNXWidth=2048 DmaxNXHeight=1536

### 2.24.2.5 AWS Client configuration for CPACS integration

In case of hybrid integration between AWS and CPACS, it is necessary to modify the AWS Client files. This is needed because CPACS might be blocking specific processes like solo.exe.

On the Client PC where AWS Client is installed, go to the solo folder:

(e.g. C:\Program Files (x86)\GE\AWS\_3.2\solo) and do the following:

1. Rename "**solo.exe**" file as "**solo32.exe**". Ensure that there is no more solo.exe file.
2. In **solo.vbs** file, edit with Notepad the line:  
`cmd = chr(34) & "solo.exe" & chr(34)`

and replace it by:

```
cmd = chr(34) & "solo32.exe" & chr(34)
```

3. Save the file **solo.vbs** before closing Notepad.

## 2.24.2.6 AWS Client configuration for upgrade from AW Server 2.0

1. To enable the **Close** button on the User Interface (instead of the usual **Logout** button that can be seen in the Standalone (No-integration) mode), edit the **solo.ini** file with Notepad and add the following line:

```
-Taskbar.Closebutton=true
```

2. Save the file **solo.ini** before closing Notepad.
3. Warn the IT Admin that this shall be done for each Client PC

**The Client configuration is complete.**

**Proceed to 2.27 Job Card IST015 - Final Settings on page 292**

## 2.25 Job Card IST014B - Seamless Client PC installation and Tests

This Job Card applies to the installation of Clients for the Seamless integration.

**For installation of Clients for Standalone (Non-Integrated) AW Server or for all other integrated AW Server, please refer to 2.24 Job Card IST014A - Standard Client PC installation & Tests on page 270.**

### 2.25.1 Client Installation Procedure

#### 2.25.1.1 Pre-requisites - Universal Viewer Client installation

Prior to be able to install the AWS Client, the Universal Viewer must be installed.

**Refer to the PACS documentation for detailed installation steps.**

**Refer to the Universal Viewer Installation Manual.**

Installation of the U.V. PACS client consist of:

- Launching an Internet navigator as Administrator. The detailed list of Internet Explorer compatible with UV client is provided in UV manuals. For information, the IE currently compatible for UV 6.0 SP3 are: IE8 32 & 64bit, IE9 32 & 64bit, IE10 32 & 64bit, IE11 32 & 64bit, and IE12 32 & 64bit (compatibility mode only).
- Making sure Active X settings are correctly configured in Internet Explorer.
- Connecting to the U.V. PACS server Web page URL (I.e: <http://3.70.211.201>) and accepting the security message by clicking on "Continue to this website (not recommended)".
- At the Centricity PACS Universal Viewer login page, log in.
- Clicking OK at Update in progress message. The message window "Update: downloads\X;X.X.XXXX\MivSetup" displays and when done, the Universal Viewer patient list displays
- Opening an exam and check that images are displayed.

#### 2.25.1.2 AW Server Client Installation Procedure

### 2.25.1.2.1 System requirements

Minimum hardware and software requirements for the client are listed on the AW Server login page.

### 2.25.1.2.2 Installation rules

#### NOTICE

DO NOT install client software on more than one client pc per customer! NO EXCEPTIONS!

The GEHC customer contract specifies that GEHC will install AW Server software on only ONE client, for the purposes of testing the AW Server system upon installation. If a GEHC FE installs and/or configures the software on more than one client per customer, IT CAN CREATE SERIOUS LEGAL AND REGULATORY PROBLEMS FOR GEHC. Except for the first client (which is set up by the GEHC FE), THE CUSTOMER MUST INSTALL AND CONFIGURE THEIR OWN CLIENTS.

### 2.25.1.2.3 Installation requirements

You need to have access to the Universal Viewer server

### 2.25.1.2.4 Client Installation Errors/Problems

It is not possible to anticipate ALL potential site security, filters, and firewall rules for this product.

Make a note of any errors in the client installation process, because they might be related to PC and/or network security / firewall configuration.

**Client problems are the responsibility of the customer!**

### 2.25.1.2.5 Standard Installation procedure

The installation of AWS Client shall be done in two steps :

#### First step - Universal Viewer Server (PACS):

The first step will consist in moving all files to the necessary locations to ensure automatic SoloMini client installation.

This will need to be done on the Universal Viewer Server only once. Refer to the *Centricity Universal Viewer with Partial CPACS Integration Installation and Upgrade Manual*.

Repeat this step when the AW Server has to be upgraded, as the AWS client has to be upgraded too.

#### Second step - Universal Viewer Client:

We will login to the Universal Viewer Client PC. Then the AWS will be automatically downloaded and installed if needed. To be done on one Client by the FE. (It will have to be done once for each Client PC. This will be the responsibility of the customer)

- 1.)     • Close any open Universal Viewer Client session.
- 2.)     • Open an Internet browser and connect to the IP address of the Universal Viewer  
I.e: <http://3.70.211.201>
- 3.)     • Login to the Universal Viewer Client (example account: **image / IMAGE**)

4.) Configure the 3D Applications button if needed.

The following has to be done for each type of exam (CT, MR, etc...) that will be associated with the AW Server 3D viewer.

- From the Worklist, open a CT exam
- Click on **Layout >> Create / Edit** in the upper panel
- Click on **Menu >> select Modality >> Click Edit button**
- Scroll up to "3D Applications" in the list and click on the "<<" sign to add in "Menu Content" window
- Click on **Save** button
- Repeat the steps for other supported modalities (MR, PET and potentially XA). This will add a "3D Apps" button in the upper panel of the U.V. PACS Client for each exam type previously customized.

**NOTE**

If the "3D Apps" button in the upper panel of the U.V. PACS is greyed, it means that there were problems at installation or that the Integration configuration parameters are not appropriate.

5.) • Close the configuration menu

6.) • Select a protocol from the 3D applications drop-down list.

The download of AWS client installer automatically begins and a progress bar is displayed.

When download starts, a Firewall popup window is displayed asking to allow access, then a "certificate accept" window is displayed.

Once download is finished, the installation of AWS Client proceeds in background.

Then the AWS client starts.

7.) • Check that the AW Server Client is properly installed:

- In the Windows Explorer, open the Folder C:\Program Files (x86)\Integrad.3\MIV\
- Verify that there is a Solomini folder
- Double click to open the Solomini folder
- Check that there is a folder with the AW Server release name (I.e: 3.2-X.Y-Z where X is the Extension number, Y is the sub extension number, Z is the build number)

**NOTE**

If you cannot find this folder, proceed with the workaround described in the following work-around step.

8.) **Workaround Step** (optional step if folder with AW Server release name does not exist)

- In the client workstation, you need to change the Admin rights of the following folder:  
C:\Program Files (x86)\Integrad.3\MIV\
- Right-click on the folder in Windows Explorer to display its Properties
- Select the **Security Tab**
- Select **Edit > Add**
- Depending on your *Windows TM* language settings, enter the correspondence to "Everyone" (I.e: for France = "Tout le monde") in text box on the Groups page
- Click **OK**
- Check **Full Control**
- Click **OK**

9.) • When done, exit from the Universal Viewer client.

## 2.25.1.3 Linux Client installation Procedure

**NOTICE**

Installation on Linux Client is NOT currently supported with Seamless Integration.

## 2.25.2 Client (System) Test

## 2.25.2.1 Client Test (summary and client information)

### Client Worklist Browser Test

This procedure is a basic “launch-and-go test” to validate basic server operation.

- 1.)  • Start the Universal Viewer Client and open an exam from the list of exams.
- 2.)  • Select the 3D applications button, then select one of the available protocol, for example "Reformat"  
The AWS Client Window should open.
- 3.)  • Experiment briefly with some of the tools and controls and verify that they respond as expected.  
(See the User Manual for details.)
- 4.)  • Click on Review steps and select **Protocol List**, then **Protocol Page**.
- 5.)  • Select another Protocol and check that it is correctly displayed.
- 6.)  • Exit the AWS Client Window by clicking the button in the left-bottom part of the window
- 7.)  

Exit the Universal Viewer Client. Click on the icon as shown.

This completes the basic operational validation test. If all steps passed successfully, the system is operating correctly.

#### NOTICE

If any of the preceding steps produced error messages or made the display hang or display artifacts, this system validation test has failed, and the system is NOT ready for customer use. Read the “Validation Test Failure – What to do” and “Troubleshooting Tips” in the following paragraphs.

## 2.25.2.2 Validation Test Failure – What to do

In the event of system validation test failure:

- Examine error(s) and corresponding error logs using the Log Viewer in Service Tools.
- Re-run the StandAlone diagnostic process.
  - If it passes, there could be network-related or client-related issues.
  - If it fails, pursue the suggestions in the standalone diagnostic section of the AW Server Service Manual.

Other suggestions in the event of system validation failure:

- Remove and then re-install the advanced application(s) package(s) using the Version Management tool in Service Tools. (Reference the Service Tools section of the AW Server Service Manual.)
- Reload both the OS and platform software (Load From Cold).

### Validation Test Troubleshooting Tips

If you cannot perform the “Installation Validation Tests” successfully, troubleshoot the component that is failing. See examples below:

- If you cannot connect to the server web page, troubleshoot connectivity-related issues:
  - Can the PC access other resources on the local network (LAN)?
  - Can the PC access the Internet?
  - Is the PC configured correctly on the network with a valid IP address, netmask/network prefix, and gateway?

- Is there an Internet proxy configured in the browser?
- Does this PC require a proxy to be configured?
- Remember, a proxy allows an internal network PC a gateway to an external network (like the Internet). If the browser attempts to use this proxy to access an internal network resource – like the AW Server – it will not be able to find it. Conversely, if the PC needs a proxy to get from the network it is on, to a remote network (like the Internet), and there is no proxy configured, the PC will not be able to connect.
- Proxy configurations should be discussed with the site IT admin. For test purposes, they can be turned off or on to see what the effects are. BUT, doing so could result in other network resources becoming non-functional until the proxy settings are returned to normal.
- Use “ping” and “traceroute” to test and verify the network functionality. The Service Tools --> Diagnostic --> Test --> Network tool does some of this for you.
- Try to narrow the connectivity issue down to either a CLIENT issue or a NETWORK issue. A good way to do this is to test multiple clients on the same subnet. If they all act the same on the same subnet, chances are there is a network issue. If only one has the problem, focus on it.
- IT IS ALSO VERY HELPFUL TO PERFORM A SIDE-BY-SIDE TEST USING A DUAL-CORE PC, SUCH AS A GEHC SERVICE/SALES LAPTOP. This is especially useful for “performance” issues, to determine whether or not the client PC is the problem, and to validate the server.
- Remember, the NETWORK and the CLIENT (other than installing AW Server client software on ONE customer client as specified in the contract) are NOT the responsibility of GEHC. Once the server is proved to be working correctly, and that the problem resides with the network or the client, the AW Server service model is validated, and the final resolutions for issues related to the network or client belong to the customer.

**This completes the AW Server Installation process.**

Once the system passes these validation tests, it is ready to be turned over to the customer for applications training and/or normal use. This is described in the next Job Card.

#### **NOTICE**

Please remember to log only actual installation time against the server’s installation dispatch. Use TRAINING (or another appropriate account) to log ‘observation’ or ‘non-installation’ site AW Server activities. Also make sure to include in the installation dispatch the “completion” comments: "HW verification complete prior to software install"

#### **2.25.2.3 Printing tests**

Printing tests are not applicable for Seamless Integration, as the AW Server Client is part of the Universal Viewer Client

#### **2.25.2.4 Client Monitor screen resolution setup**

Client Monitor screen resolution setup is not applicable for Seamless Integration, as the AW Server Client is part of the Universal Viewer Client

The Client configuration is complete.

**Proceed to [2.27 Job Card IST015 - Final Settings on page 292](#)**

### **2.26 Job Card IST014C - Web Client Tests**

The Web Client is a web-based client that allows to start the AW Server advanced applications using a web browser. It is an alternative to the AW Server Client software.

**NOTE**

The Web Client is available for Standalone (Non-Integrated) AW Server.

**NOTE**

The Web Client requires a license to be activated. Refer to [2.15.10.5 Flexera licensing on page 162](#).

**NOTE**

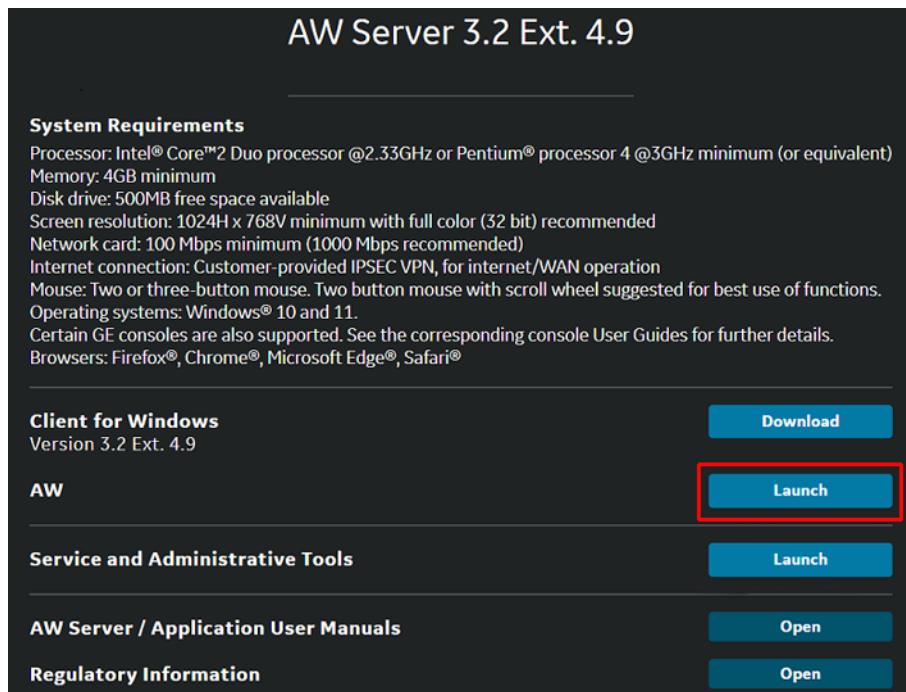
The Web Client requires the Imaging Cockpit Components to be installed and the Web Client to be activated. Refer to [2.16 Job Card IST017 - Imaging Cockpit Components Installation on page 167](#).

The below test allows to validate the AW Server installation as a system by connecting to a client PC via the site's network and performing basic tests of the Web Client.

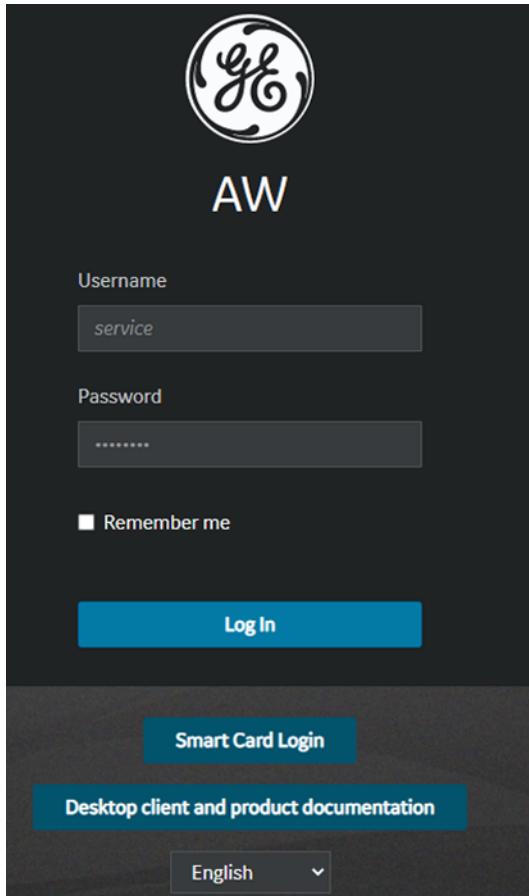
1. At the Client PC, open a web browser and type in:

`https://<AW_server_IP_address>/`

2. If not already done, accept the cookies in the window that popups.
3. In the landing page, click on **AW Launch** button.



4. The login screen appears.

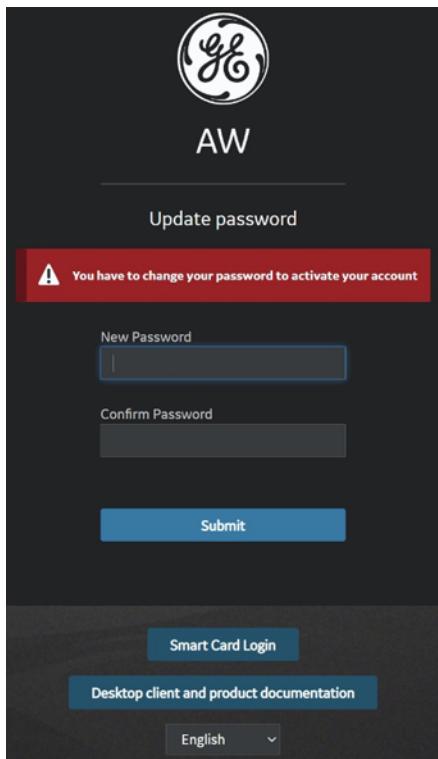


5. Login using a valid local AW Server account and password, or a valid enterprise account name and password.

#### **NOTICE**

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.21 Job Card IST006 - Changing the Passwords on page 249](#) for the password change guidelines.

## 6. The Web Client Worklist Browser appears.

It displays exam datasets, advanced applications launch buttons (when applicable), and remote DICOM host queries, among many other functions.

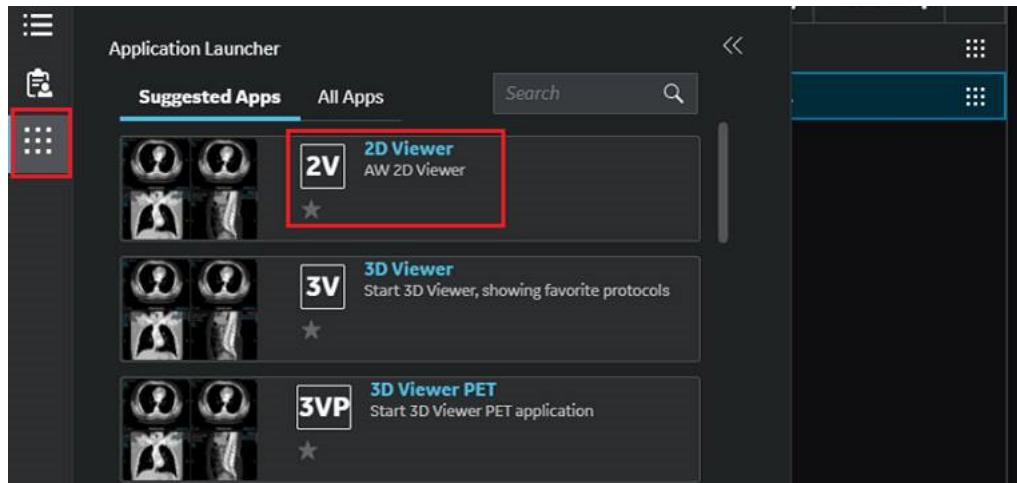
Patient name	Patient ID	M...	Study description	Study ...	Accessio...
SSF_Demo_Exam_03	AW109705...	CT		Jan 1, 2012...	...
Demo, CT Cardiac	AW610206...	CT	ANONYMIZED	Sep 21, 200...	...

- Select an exam from the list of exams in the browser, then select a series image-set in the Series List. The Image preview window (at lower right) should display an image from the selected series, as in the example shown above.

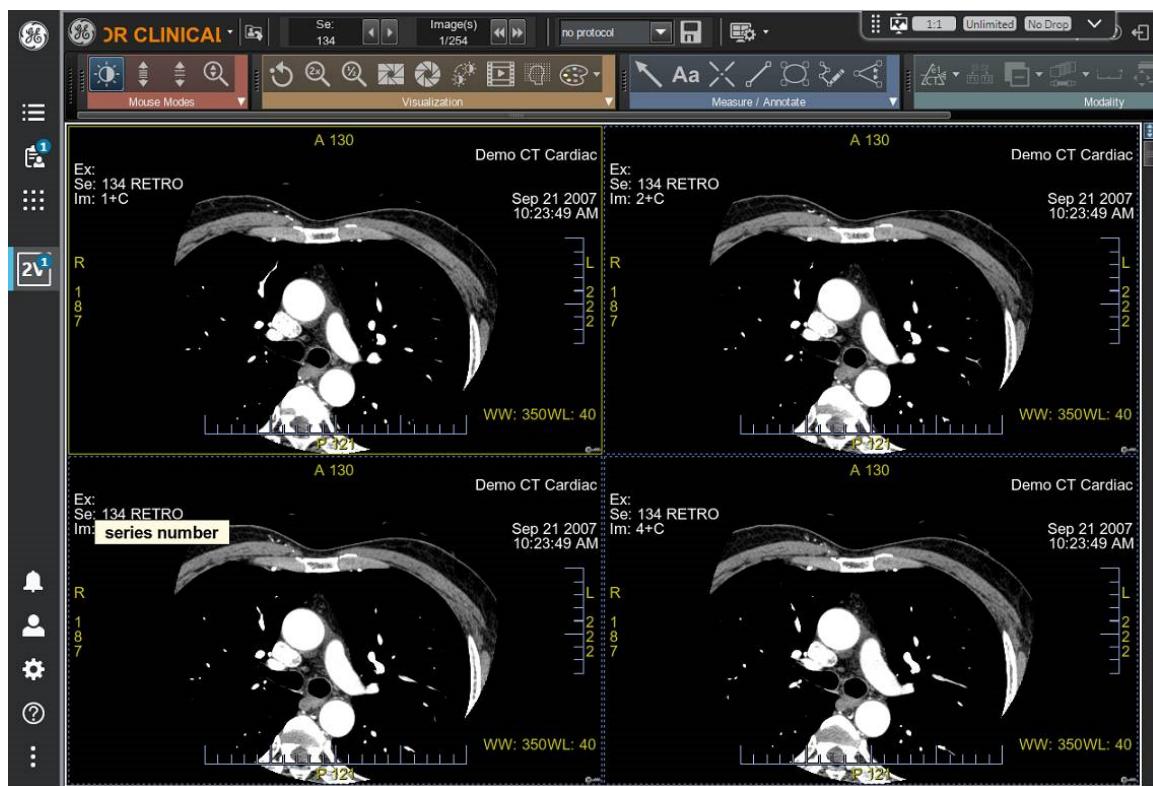
**NOTE**

An exam source should be configured before any exams will be listed. Refer to [2.18.1 Configuring DICOM hosts in Service Tools on page 184](#).

- From the Application Launcher menu, click on **2D Viewer**.

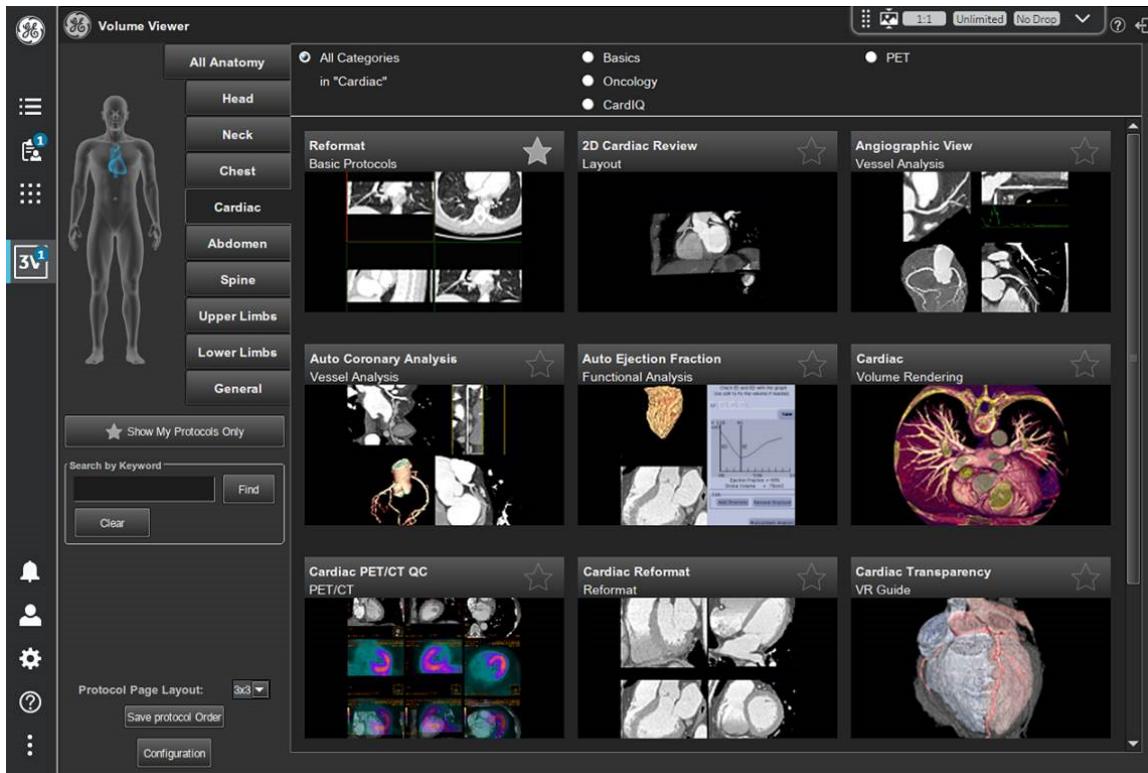


- The 2D Viewer application should launch as shown below:

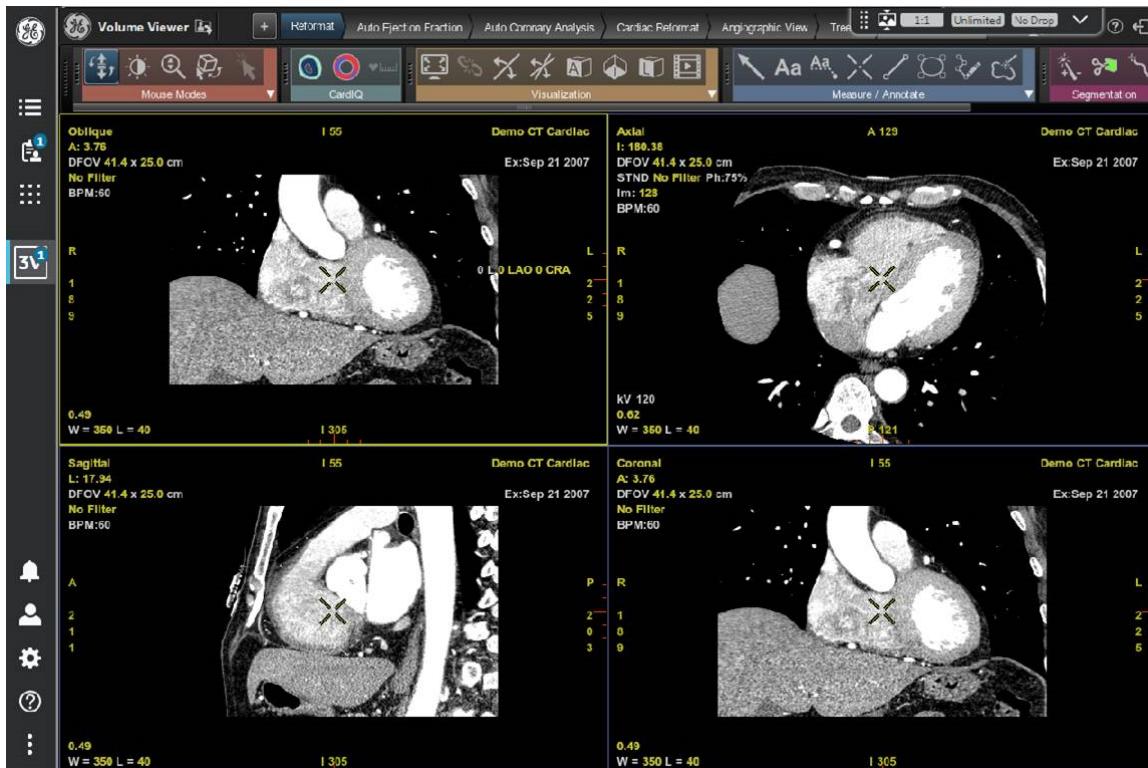


- Experiment briefly with some of the tools and controls and verify that they respond as expected. (See the User Manual for details - Available from the landing page – Type in a new tab in the web browser: [https://<AW\\_server\\_IP\\_address>/landing/](https://<AW_server_IP_address>/landing/) and click on **Open** for the AW Server / Volume Viewer User Manuals).
- Click on exit (at the upper right) to close the 2D Viewer.
- From the Application Launcher menu, click on **3D Viewer**.

13. The 3D Viewer launches and splash screen should display, then the protocol selection and tool frame should come up as shown in the following illustration.

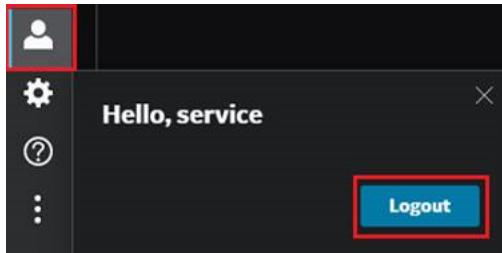


14. Click on one of the protocols (for example, “Reformat”). The “Reformat” screen displays as shown below:



15. Click on exit to close the Volume Viewer. The display should go back to the exam list and series image display.

16. Logout the Web Client. From the Personal menu, click on **Logout**.



#### NOTICE

If any of the preceding steps produced error messages or made the display hang or display artifacts, this system validation test has failed, and the AW Server is NOT ready for customer use. Read the [2.24.2.2 Validation Test Failure – What to do on page 279](#).

## 2.27 Job Card IST015 - Final Settings

You will now go through the final settings prior to handing over the AW Server to the customer. It is advisable that one person representing the customer (preferably an IT administrator) go through this Job Card with you.

### 2.27.1 SNMP setup in iLO Service processor

#### NOTE

If the Secured for RMF mode is planned to be activated, then do not perform this procedure, keep SNMP in Disabled state. SNMP feature is not supported in RMF mode

In order to have the Hardware related traps caught in a log file on the AWS side (/var/log/snmptraps.log), it is necessary to configure SNMP in the iLO service processor of the AW Server.

#### 2.27.1.1 Pre-requisite for using with Prodiag

Not applicable for Seamless integration and Secured for RMF mode.

- RSvP is configured (see [2.15.2 Remote Service on page 141](#))
- SNMP is configured in the AW Server (see [2.15.8 Configuring SNMP on page 151](#))
- The iLO service processor is configured and operational
  - It is mandatory to have declared the Gateway for iLO.
  - The IP address of the iLO must be in the same subnet as the server IP address.

#### NOTE

Prodiag is configured by default to check on the existence of the /var/1og/snmptraps.log file once a day. If the file has a content (other than the default opening line), then Prodiags sends the log file to GE backoffice. Prodiag can only send the log file if the system is RSvP configured. Also note that Prodiag is configured by default to send with no delay any software reported issue. Prodiag is configured by default. (For more information, see [2.15.2.1.3 Prodiag configuration on page 145](#))

#### 2.27.1.2 SNMP setup in the iLO 5 service processor

This procedure details the steps for iLO 5. For iLO 4, iLO 3, refer to [A.7 SNMP setup in the iLO service processor on page 588](#).

1. At the Client PC or FE laptop, open a browser (Firefox or Internet Explorer) and type in the AW Server's iLO Service processor IP address.

I.e: <https://3.249.14.161/>

2. When the login page loads, login as **root**.
3. When the iLO page loads, select **Management > SNMP Settings**.

The screenshot shows the iLO 5 management interface. On the left is a sidebar with various navigation options: Information, System Information, 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, Management (which is selected), and Intelligent Provisioning. The main content area is titled "Management - SNMP Settings". It has three tabs: "SNMP Settings" (selected), "AlertMail", and "Remote Syslog". Below the tabs is a section titled "SNMP Settings" containing fields for "System Location", "System Contact", "System Role", "System Role Detail", and "Read Community 1". At the bottom right of the main content area are several small icons: a green circle, a blue circle with a dot, a yellow triangle, a red shield, a person icon, and a question mark.

4. Scroll down to **SNMP Alerts** and check that **iLO SNMP Alerts** and **Cold Start Trap Broadcast** are enabled. If they are not enabled, enable them then click on **Apply**.

## SNMP Alerts

This screenshot shows the "SNMP Alerts" configuration page. It includes the following settings:

- Trap Source Identifier:** A radio button group where "iLO Hostname" is selected, while "OS Hostname" is unselected.
- iLO SNMP Alerts:** A toggle switch that is turned on (green).
- Cold Start Trap Broadcast:** A toggle switch that is turned on (green).
- Periodic HSA Trap Configuration:** A dropdown menu set to "Disabled".

At the bottom are two buttons: "Send Test Alert" (in a green box) and "Apply".

5. To enter the SNMP Alert Destination, scroll down to **SNMP Alert Destinations** and click on **New**.

## SNMP Alert Destinations

Alert destination not configured.

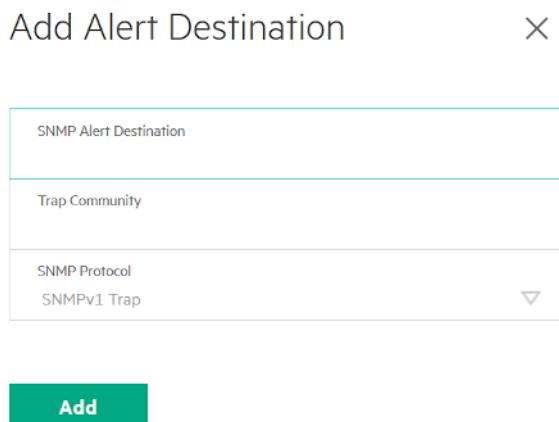
**New**

**Edit**

**Delete**

6. In **SNMP Alert Destination**, enter:

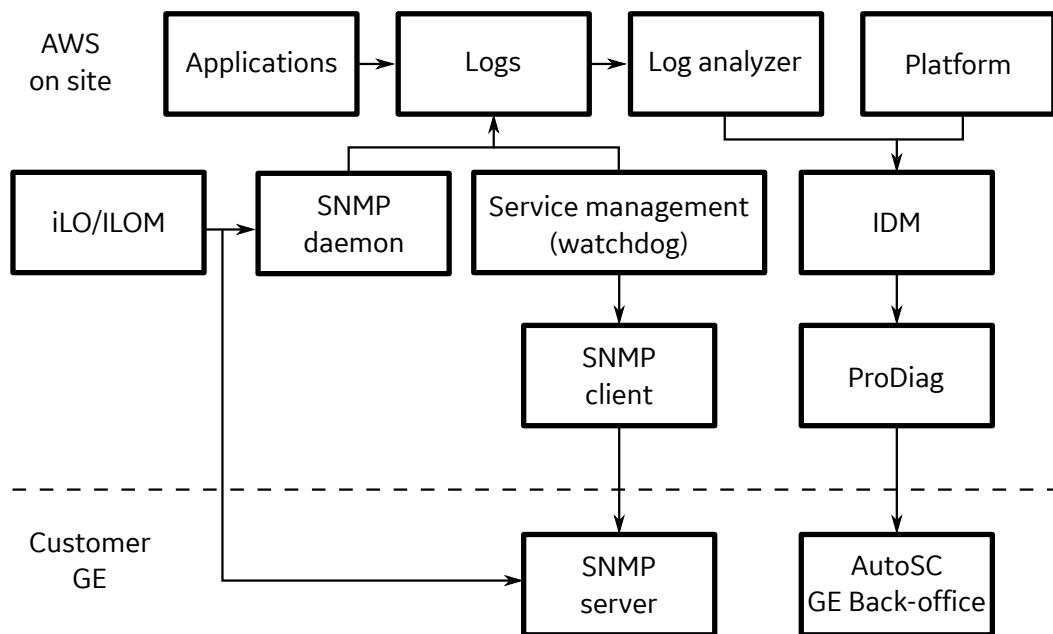
- the site's SNMP server IP address if there is any,
- or the AW Server IP address.



- Click on **Add**.
- To send a test alert to the setup destination logfiles, click on **Send Test Alert** in *SNMP Alerts*.
- Launch the Terminal from the **Service Tools > Tools** and check the `/var/log/snmptraps.log` file.
- Logout from the iLO Service processor.

### 2.27.1.3 Service Workflow

The following is given for your information only, in order to point out the main differences between the DI and IT organizations workflow for SNMP traps management.



### 2.27.2 Anti-Virus setup

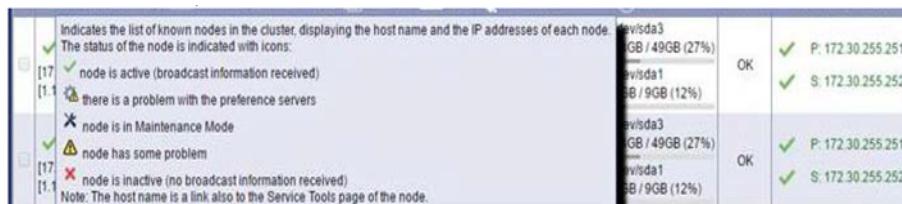
During Secured for RMF mode activation the AW Server will automatically setup and activate McAfee anti-virus software. Refer to [2.31 Secured for RMF mode on page 448](#).

In non-RMF aka Generic mode, if the site requires to set up the **ClamAV anti-virus**, refer to [A.5 ClamAV® on page 575](#) for instructions.

## 2.27.3 Scalability (cluster) mode operation verification

If applicable to your site, verify now that all the virtual AW Servers setup for cluster mode operation show up as "mode is active" in the cluster, that one of them is setup as "preference server for the cluster" and is active, and that none of them has been left in Maintenance mode for instance.

Also check that the "node has some problem" icon does not show up, unless only one external license server has been setup for your site.



## 2.27.4 Hard disks serial numbers

The `/var/tmp` folder contains a `disk_sn.out` file created at time of installation, containing the serial numbers of the disks of the server.

This list is aimed to collect at time of installation, or at later time upon replacement of any of the hard disks, information on the serial numbers of all the hard disks while they are operational and able to send information. **It is recommended to save this list of serial numbers for future use.**

If at a later time, your system gets one or more defective hard drive(s), the hard drive(s) may no longer be able to reply to a request and send information on their serial number.

When contacting HP support center for getting replacement hard disk drive under warranty, the serial number of the defective disk(s) will be requested by HP support.

Having the serial number on a list will allow you to know the serial number of the disk(s) that are no longer able to send a reply, so you can communicate it to HP support.

### 2.27.4.1 At installation time

Open a Terminal tool and type in:

```
cd /var/tmp <Enter>
cat disk_sn.out | grep Serial > /export/backup/HDDSerial<Date> <Enter>
I.e: cat disk_sn.out | grep Serial > /export/backup/HDDSerial20150813 <Enter>
```

You may also copy the file on the Client PC, or FE laptop, and/or any USB device.

You may also want to write down in the Site's maintenance logbook those serial numbers.

### 2.27.4.2 After hard disk drive replacement

You must update the `/var/tmp/disk_sn.out` file with the replaced HDD(s) serial number(s).

- Open a Terminal and type in to generate the new list of serial numbers:

```
/usr/local/bin/gener_list_diskSN <Enter>
```

- Proceed with steps described in [2.27.4.1 At installation time on page 295](#) to store the updated HDD serial numbers list for future use.

## 2.27.5 PNF Firewall setting

The Server is exposed to a Security Risk if the PNF Firewall is turned Off.

Malicious users can login via SSH and access, corrupt, or delete sensitive files.

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

- To check the status of the PNF Firewall from the Service Tools, connect to the Server's Service Tools Web page. Check the Firewall (pnf) status in the Health Page:

Software Subsystem	Status
Image Management Subsystem (nuevo)	OK
Firewall (pnf)	OK
Audit Server (ea1)	OK
Authentication/Authorization Server (ea3)	OK
Application interoperability platform (dotmed)	OK
Super Server (aweservice)	OK

The status should appear as "OK" on a green background.

- If the Firewall is not active, contact the local IT to see if it was intentionally turned Off. If not, you must turn it On:
  - In the Service Tools, go to **Tools > Terminal** menu.
  - Click the **New modal Terminal** button to open a command window.
  - In the Terminal Window, login as user **root**.
  - Type in the following command to enable the Firewall:  
**systemctl start pnf <Enter>**
- Go back to the Server Healthpage and make sure that the Firewall is now ON.

### NOTE

A mechanism has been implemented which keeps PNF Firewall turned ON. A daemon process check the PNF status and, if needed, switch it to ON on a daily basis. However, if you find that the PNF Firewall is not active, apply the above manual procedure.

## 2.27.6 Media Creator

Media Creator allows you to write exams/series/images to a selected USB media or CD/DVD.

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.

To check the status of the Media Creator from the Service Tools, connect to the Server's Service Tools Web page. Check the Media Creator (mediacreator-app) status in the Health Page:

Smart Card Login (tomcat-smartcard)	OK
Media Creator (mediacreator-app)	OK
Configuration Service (configuration-service)	OK

The status appears as **OK** on a green background.

## 2.27.7 Volume Viewer performances on VM

This section only concerns AW Server running on virtual machine.

**NOTE**

**Hyperthreading needs to be turned off** on the Hypervisor to optimize the performances of the AW Server and the 3D applications. Indeed, the software is optimized for CPU settings with Intel Xeon architecture and without hyperthreading. So, it is recommended to deactivate the Hyperthreading on AW Server. Therefore, it is not appropriate to have other customer's VMs running on the same Hypervisor, if these other VMs require Hyperthreading to be activated, otherwise it could impact the AW Server performances.

**NOTE**

In that case, Volume Viewer 3D performances may be improved by configuring the number of active threads as follows.

- To do this setup, open a Terminal, login as **root** and edit the file with the "vi" editor or any suitable editor such as "nano":

**vi /export/home/sdc/vxtl/bin/start\_volan <Enter>**

- Add the following line at 3rd position in the file:

**setenv VXTL\_NUMCPUS XXX** (where XXX is either 4 or 12)

I.e: setenv VXTL\_NUMCPUS 4

where XXX is the number of physical cores available for the Virtual machine. This number XXX is usually half the number of cores available for the Virtual Machine:

- For Low Tier virtual machine (8 virtual CPUs) >>> set XXX= **4**
- For High Tier virtual machine (24 virtual CPUs) >>> set XXX= **12**
- Save the file and quit the editor

**NOTE**

This configuration must be re-applied each time the Volume Viewer application is re-installed.

## 2.27.8 For China only - CFDA Registration documents

In China, a regulatory requirement states that Platform/Applications CFDA Registration documents shall

be available on client site. When appropriate, they will be delivered with the product, either in paper format or electronically on the CFDA Doc addendum media.

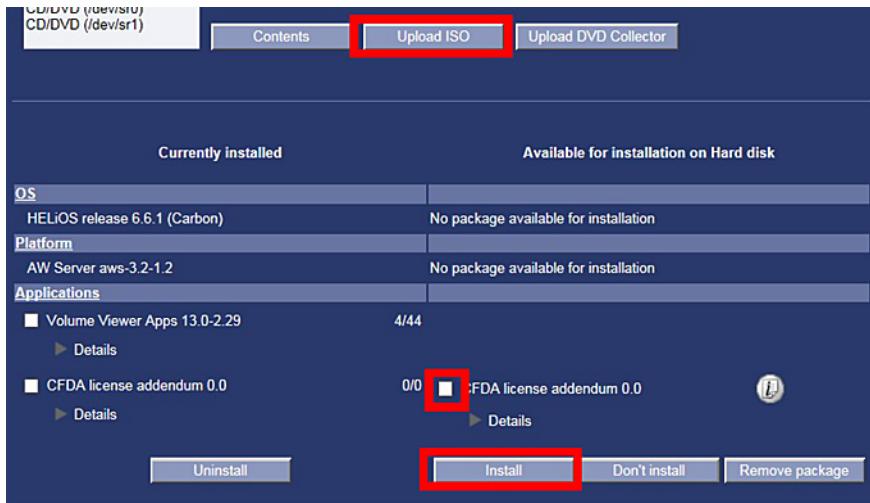
- If CFDA Registration documents are delivered on paper, they must be given to the client and be securely stored on site in case of an audit.
- If they are delivered on a media, they must be installed on the AW Server, following the procedure described below.

### 2.27.8.1 Installation on server

Each time the AW Server platform will be installed or reinstalled (Load From Cold), the CFDA Doc addendum will have to be installed as well.

If the platform/applications release changes (in case of Upgrade), the CFDA Doc addendum will have to be updated. Make sure to always install the latest available version.

- Refer to Job Card IST009 [2.17.2 Load the Application\(s\) from media on page 174](#) instructions, to install the CFDA Docs addendum from its media, in the same way you install an Application, through the *Version Management* tool.



1. Insert the media into the CD/DVD drive of the Client PC (or insert the USB device into the USB port) and click **Upload ISO** button. Select the file (*Browse*) and click **Send to system** button.
2. When the package is uploaded, it shows up in the "*Available for installation on Hard disk*" section. Select the package (click on the radio button) and click on the **Install** button.
3. When done, check under the **Documentation / Documentation** tab, that the CFDA addendum doc(s) are available in the User documentation section (select language = Chinese)

## 2.27.8.2 Upgrade

- To upgrade the documents to a newer version, you shall first uninstall them and then install the new revision following the procedure described in [2.27.8.1 Installation on server on page 297](#)
- To remove the document package from the disk, proceed as follows:
  - Remove the documents: Click on the Radio button in the *Currently installed* section, then click on the **Uninstall** button.
  - Remove the package: Click on the Radio button in the *Available for installation on Hard disk* section, then click on the **Remove package** button.

### NOTE

Other countries: Discard the CFDA doc addendum media.

**The final configuration is complete.**

Proceed to [2.28 Job Card IST016 - System Handover to Customer on page 298](#)

## 2.28 Job Card IST016 - System Handover to Customer

You will now go through the procedure to handover the AW Server to the customer.

It is REQUIRED that at least one person representing the customer (preferably an IT administrator) go through this Job Card with you.

Explaining these items correctly and thoroughly to the customer is crucial to a smooth handover.

As a final step, you will also show the customer how to do a configuration backup.

## 2.28.1 Installation handover tasks - Handover Checklist

When transferring the AW Server system to the customer, it is important to inform the customer – especially the site IT administrator person(s) – what their expectations should be regarding the following items, and where to find certain information.

Discuss the following points with the site's IT admin and/or CUSTOMER.

### **Handover information outline reference.**

- DICOM Demo exams
- Administrator guide (part of the User's guide)
- User Account Management
- DICOM Hosts management
- Failure / Repair process
- iLO information and capabilities
- Failure discovery process
- Open Source Software for AW Server
- Warranty
- Preventive Maintenance
- Applications training (see [2.28.3.1 AW Server User and IT Administration Training on page 304](#))
- 3rd Party certificate

#### **1. DICOM Demo exams**

##### **NOTE**

Bypass this step for Full, Seamless or DICOM Direct Connect Integration. The DICOM demo exams installation is not applicable to Full, Seamless or DICOM Direct Connect Integration, as no image data can be loaded to the AW Server image database.

For the purpose of system testing, demonstration, and training there is a demo 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 media, together with more demo exams, from the Client User Interface, using the Tools/Free Image Importer. Refer to the AWS User guide for more precise details.

##### **High level workflow:**

- Launch the AWS Client from the Client PC
- Insert the AWS Demo Exams media into the Client PC
- Click on Tools tab
- Click on Free Image Importer.
- Click on Import more images
- Select the media
- Search for the compressed diagnostic images file and click open to start importing images.

#### **2. Administrator guide**

- Go to Service Tools > Documentation > Documentation, click on Documentation button. 2 tabs open. In the tab containing the User guides, the AW Server Administrator Guide is available.
- Another way to obtain the Administrator Guide is to go to the AW Server home page in an internet browser, then click on "Open" next to "Operator Manuals" and "AW Server/3D Viewer/2D Viewer/Volume Viewer".

### User Account Management

- The GEHC FE will help the IT admin to configure one or two accounts or the Enterprise server configuration during system turnover. But, the complete or ongoing user account creation and management is owned by the customer's site IT ADMIN or equivalent operative.

### DICOM Hosts Management

- The GEHC FE will help the IT admin to configure one or two DICOM hosts during system turnover. But, the complete and ongoing DICOM hosts creation and management tasks are owned by the customer's site IT admin or equivalent operative.

### Preferences Management

- The GEHC FE will help the IT admin to configure the Preferences User-share menu under Service Tools / Tools sub-menu.

## 3. AW Server Failure / Repair Process

Refer to the AW Server Service Manual for details on Break/Fix process.

All requests for service should be through the GEHC service request process.

The GEHC failure and repair model covers two basic points, hardware and software:

### Hardware

- GEHC has the wing-to-wing service responsibility to support and repair all hardware failures (or via the hardware vendor - High Tier server case).
- If needed, GEHC will dispatch the hardware vendor to repair or replace the hardware issue.
- The hardware vendor will complete the hardware repair, then turn the service call over to GEHC for follow-up and turnover to the customer.
- To maintain security and confidentiality, all replaced system IMAGE / PATIENT DATA disk drives will be left on-site or if not, use a **Disk Wipe Tool** - to permanently remove data. Refer to [3.12.6.8 Final steps on the old AW Server - Delete Patient data on page 551](#).
- All other NON-PATIENT-DATA components will be exchanged, or disposed of per the vendor's Hardware Replacement Policy for that particular part.

### Software

- GEHC has the wing-to-wing service responsibility to support and repair all software failures.

## 4. iLO information and capabilities

The iLO (HP) service processor has many service capabilities. General information for these capabilities can be found in the service manual and the vendor's technical publications referenced there. GEHC is not responsible for the full support of the iLO, or its functionality.

## 5. Failure discovery process

The AW Server hardware has redundant components that can and will fail-over to a back-up state when one of these components fails. End users will not automatically know if this happens. GEHC will not automatically be alerted. The only way the failure will be noticed is when someone accesses the system service tools and / or inspects the fault LED's on the SERVER. Whenever a fault LED or FAULT ALARM is observed, GEHC should be notified immediately through the GEHC service request process.

## 6. Open Source Software for AW Server

Discuss with customer's IT and or Customer Admin designee:

Portions of this product are subject to various open source license agreements that require re-distribution of source code contributions. These contributions may be found on the media labeled "Open Source Software for AW Server."

This is a data media containing no documentation or executables that apply to the usage or service of this product. The media is included in the product structure in order to comply with open source license terms. Depending on individual site requirements, you may either store this media with other AW Server media or provide it to the customer's system administrator.

## 7. **Warranty**

Discuss with IT and or Customer Admin designee:

The AW Server is under a ONE-YEAR warranty by GEHC. All service requests must be directed to GEHC service during this period. There will be a service contract offering(s) after the ONE-YEAR warranty period. If the site decides not to purchase a service contract, the on-going service of the AW Server will be handled on a time-and-materials-and-availability model if directed to GEHC.

**HP hardware warranty is THREE years.** Refer to section [2.28.3.7 HP Care Pack Warranty extension on page 307](#) for details.

## 8. **Planned Maintenance (P.M.)**

Discuss with IT and or Customer Admin designee:

The hardware has no PM requirements specified by the vendor. However, some PM tasks such as checking the software errors are described in the Service Manual.

It is recommended that the site's IT department periodically inspect the SERVER for fault LED indications.

If a fault LED or FAULT ALARM is observed, GEHC should be notified immediately through the GEHC service request process.

## 9. **3rd Party certificate**

3rd Party certificate acquisition and maintenance is under the full responsibility of the customer.

## 2.28.2 Backup Parameters and Settings

### 2.28.2.1 Network and UPS configuration Backup

The network configuration is performed via AWS network configuration script, and IS NOT saved by the AW Server Service Tools backup process. The network configuration is considered a prerequisite, and is separate to the AW Server remote configuration and service tools.

The important information to record in the site log book (or some similar permanent record) - or access from the existing site IT records - are the following data points:

- Server IP address
- Server hostname
- Server Netmask/Network prefix
- Gateway IP address
- Site network DNS IP address(s)

The network configuration for the system was already recorded as part of the site survey process. Alternatively, ALL of this information can be retrieved from the site's IT department, in case this information is missing, not available via the system tools, or undergoing site changes.

We recommend that you backup the following files **and that you also write down the information in the Site's maintenance logbook** if not already done.

The Network and UPS parameters will be saved in the `/export/backup` directory, which is used to store the System and Users parameters.

- This is not the case for Full, Seamless or DICOM Direct Connect Integration. In this case, the backup directory is created on the system disks and will not be saved at OS reinstallation.
- This is also not the case for AWS2.0 / AWS3.0 upgrade to AW Server 3.2 release, as the filesystems will be upgraded from EXT3 to EXT4 filesystems, and consequently erased.

**Therefore, ALSO write down ALL the information in the Site's Maintenance logbook.**

- 1.) • From the Service Tools, open the Terminal (Tools sub-menu).

- Login as root:

**root <Enter>**

Password : Enter the root password

- 2.) **Network configuration**

- Save the Network configuration (create a "network.txt" file) :

**ip addr > /export/backup/network.txt <Enter>**

**cat /export/backup/network.txt <Enter>**

(to check if the appropriate info was saved)

- Save the hosts file configuration (create a "hostname.txt" file) :

**cat /etc/hosts > /export/backup/hostname.txt <Enter>**

**cat /export/backup/hostname.txt <Enter>**

(to check if the appropriate info was saved)

- Save the Routers configuration (create a "routers.txt" file) :

**ip route > /export/backup/routers.txt <Enter>**

**cat /export/backup/routers.txt <Enter>**

(to check if the appropriate info was saved)

- Save the file containing DNS parameters:

**cat /etc/resolv.conf > /export/backup/dns.txt <Enter>**

**cat /export/backup/dns.txt <Enter>**

(to check if the appropriate info was saved)

- 3.) **UPS configuration** (High tier server only)

For the HP High Tier server. Save the UPS configuration (if applicable):

- Create the UPS directory

**mkdir /export/backup/ups <Enter>**

- Stop the HPPP service:

**systemctl stop HP-HPPP <Enter>**

- Copy the configuration files

**cp /usr/local/HP/PowerProtector/configs/config.js /export/backup/ups/config.js <Enter>**

**cp /usr/local/HP/PowerProtector/db/mc2.db /export/backup/ups/mc2.db <Enter>**

- Restart the HPPP service:

**systemctl start HP-HPPP <Enter>**

- **NOTE**

The UPS configuration can be restored by reversing the above scripts:

**systemctl stop HP-HPPP <Enter>**

**cp /export/backup/ups/config.js /usr/local/HP/PowerProtector/configs/config.js <Enter>**

**cp /export/backup/ups/mc2.db /usr/local/HP/PowerProtector/db/mc2.db <Enter>**

**systemctl start HP-HPPP <Enter>**

## 2.28.2.2 Configuration Backup

You will now show the customer, how to create a configuration backup.

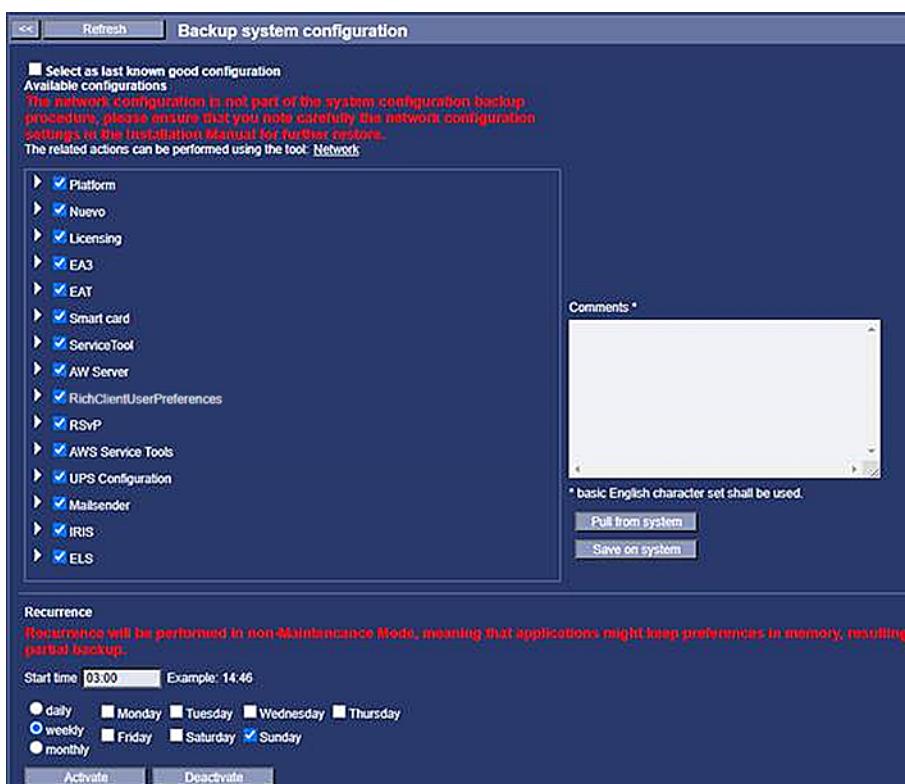
To minimize the chance of file corruptions during configuration backup, the AW Server will be placed in Maintenance Mode. If not already the case, refer to [3.5 Entering the Maintenance Mode on page 486](#).

### NOTICE

Frequent configuration backups are CRITICAL for service and troubleshooting.

- From the Service Tools, select **Maintenance > Backup > System configuration**.

The *Backup system configuration* panel appears.



- Choose a **Start time**. Use a time where the server is supposed to be on (i.e: 12:00), in case it would be regularly turned off in the evenings.
- Select a recurrence for future backups. You may choose daily, weekly or monthly.
- Click on the **Activate** button to save.

The message success appears.

### NOTE

Recurrent automated backups are performed in normal mode, not under maintenance mode, that is to say, depending on the time of the day they are scheduled, they may not contain the latest changes done by the Users.

Up to 3 Recurrent automated backups will be kept a long time. The removal of the older backup file will be automatic when the latest backup is performed.

Manual backup is not concerned and will be kept a long time, until it is intentionally deleted.

- Proceed to the immediate backup:

- Make sure all boxes are checked under *Available configurations*.

- b. Check the **Select as last known good configuration** checkbox.
- c. Click on the **Save on System** button.

The configuration is saved on the backup partition of the server. When done, the message **successful** appears.

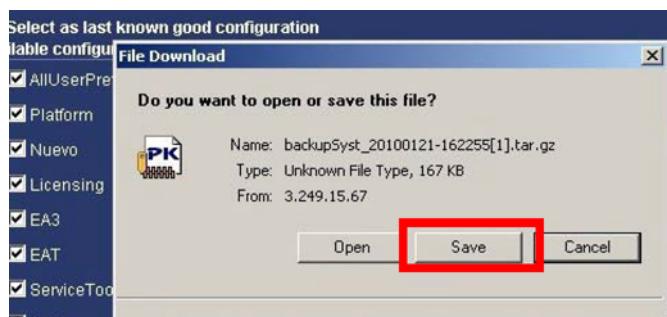
### NOTICE

For Full, Seamless or DICOM Direct Connect Integration, the backup must be made on the Client PC and/or FE laptop, as reloading the software (OS + AWS) deletes all files on the system hard disk.

- d. Click on the **Pull from system** button.

It allows to save the configuration as a .tar.gz zipped file on the Client PC (or your laptop), and transfer it later on your USB media for example.

- e. In the pop-up window, click on the **Save** button.



- f. In the pop-up window, select the destination where to save the file and click on **Save**.
6. Save the backup on a media like a USB media, for future use.

### NOTE

As mentioned in the previous section, Network parameters are not part of the backup tool. These parameters must be saved manually. In order to ease getting this information, a link to the **Network** menu is provided on the Backup and Restore tools, as shown in the illustration below.



## 2.28.3 Final steps

### 2.28.3.1 AW Server User and IT Administration Training

Applications training will be scheduled shortly after the installation. User/Client browser functionality, workflow, tools, and user account management will be topics covered by the training.

The IT admin can be trained on advanced Applications.

Refer to the Sales Team, to train the radiologists on Advanced applications.

**NOTICE**

Also recommend that the "Hibernation" feature should be turned off on Windows TM Client PCs used (also for Universal Viewer), to avoid entering into blocking timeout.

### 2.28.3.2 GIB / SIEBEL update and paperwork

Send the customer's Global Installed Base data to GEHC. Send all paperwork from the installation to the appropriate recipient (i.e., GEHC or the customer)

COMPLETE THE PRODUCT LOCATOR INSTALLATION CARDS (ICD CARDS DELIVERED WITH THIS PRODUCT) AND RETURN THEM TO YOUR PRODUCT LOCATOR ADMINISTRATION. OTHERWISE, YOUR SYSTEM UPGRADE WILL NOT BE REGISTERED IN THE GLOBAL INSTALLED BASE DATABASE (GIB)!!!

Global Installed Base database may be directly updated using the following link:

<http://gib.gehealthcare.com>

- GEHC Global Install Base database web site is available from any outside web enabled PC.
- The FE can enter the model/serial into the Service Tools interface and send the GIB data up to GIB via email. So, make sure to fill-in all the information in the service tools Initial Configuration > Device Data & User Data.

**NOTICE**

USCAN System ID / Assets are no longer found in eGib and are now located in the CRM Siebel / Assets database.

- **"Installs:** Follow MyWorkshop document DOC1701877, Job Card IB Verification
- **"Upgrades:** Follow MyWorkshop document DOC1618060, Job Card FE Upgrade Instructions
- **"Asset Swaps:** Follow MyWorkshop document DOC1589267 Job Card FE Asset Swap

**NOTE**

EDS US remains on GIB until further notice

### 2.28.3.3 Register High Tier Server with Genpact

Make sure you have completed this step described in the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware), section *Register the Server with Genpact* in order to send the hardware details (GON Number, GE Server Part Number, Vendor Server Serial Number, Customer Site Name, etc..) to the Genpact organization.

### 2.28.3.4 Capture the UDI number in Service Records

Regulatory agencies are requiring a **Unique Device Identification** (UDI) system to adequately identify medical devices through their distribution and use.

AW Server Medical Device UDI is available for each platform Software release.

**NOTE**

There is no UDI for Advanced Applications when installed on AW Server. There is no UDI for standalone Hardware.

1. Capture the AW Server 3.2 UDI, REF and LOT numbers in the Service Records, according to the process in place in your pole.

The UDI is available from the AW Server 3.2 Main page.

The UDI, REF and LOT are available from the *HealthPage* and are contained in the Configuration file.



System Configuration	
System ID	AWBUCLAB243
Platform version	aws-3.2-4.0-2038.3-32ef1913
Hostname / IP Address	bucaw70-243 / eth0: 3.249.70.243
Encrypted (TLS) AET / Port	bucaw70-243 / 2762
Plain AET / Port	bucaw70-243 / N/A
CPU (8)	Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Operating System	HELIOS release 7.7 (Nitrogen)
OS Version	7.7
Modality OS Version	AWS3.2_OS_6.0-2037.1-0acb3982 [20200907]
UDI	(01)00840682102384(10)AWS3D2E004D0
REF	5719780
LOT	AWS3D2E004D0
Uptime	1:13

### NOTICE

A distribution UDI value and bar code are printed on the AW Server SW & Docs media. It is not the Medical Device UDI. Do not scan or record this value in the Service Records.

Configuration file output example showing UDI information:

- To avoid transcription errors, extract the UDI value from the Configuration file. This allows you to copy it from the file and paste it in the Service Records.

Click on the **Display** button under the *Configuration and status* section.



Under the STATION CONFIGURATION section, the UDI, REF and LOT numbers display.

For example:

- UDI : (01)00840682102384(10)AWS3D2E000
- Medical Device Item number [REF] : 5719780
- Medical Device Production [LOT] : AWS3D2E001D0

### 2.28.3.5 Print the AWS Configuration

Display the HealthPage and under the Configuration & status tab:

- Click on **Pull from system** button. This will save the AWS configuration as a zipped file.
- You can copy it to your USB media for example.

- Unzip the file and print it with one of the Postscript printers setup for the Client PC you are using at the moment.
- Leave the print attached to the Maintenance logbook or to the paper copy of the Installation Manual.

### 2.28.3.6 Customer Release Note and information

Deliver the CRN (customer release note) if any, to the customer.

### 2.28.3.7 HP Care Pack Warranty extension

To be done for HP High Tier server only:

Notify the customer that the HP Care Pack warranty will expire in 3 years, and that they will directly receive notification from HP, to ask if they wish to pursue the support contract from HP for the hardware.

#### **NOTICE**

The customer is responsible for renewing the Care Pack contract with HP after the warranty period. Refer to the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware), section *Register the Server with Genpact*.

### 2.28.3.8 PSI code verification

Check that the PSI code in the database is appropriate, and if not, contact your Support Center to have it corrected:

- **I for EDS**

I.e: *IAWV32*for virtual AW Server 3.2

- **C or W for HCS**

I.e: *CAWH01*or *CAWH02*for High tier physical server

*CAWL01*or *CAWL02*for Low tier physical server

*CAWV32*for virtual AW Server 3.2

### 2.28.3.9 Site Cleanup

Clean up any debris left from the installation and testing process.

Make sure to appropriately dispose/recycle the useless cables.

## 2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink

The AW Server can be integrated within the CT/MR Console Environment within the CT/MR Smart Subscription on Edison HealthLink (EHL).

It allows console users to do advanced processing with AW Applications remotely.

In these environments, the installation procedure is common for CT and MR.

- For CT, the AW Server Client is installed on the CT Console.
- For MR, the AW Server Clients are installed on the customer desktops/laptops.

The OS, the AW Server software and the applications are common for CT and MR (for sure the specific modality applications are installed only on the corresponding environment), and are installed in a virtual environment.

The OS and AW Server software are packaged in a pre-installed image delivered on USB device and used to install and configure the AW Server.

The AW Server is configured in the DICOM Direct Connect mode and retrieves the patients/images data from the CT/MR Console database.

#### **NOTE**

Always refer to the relevant service documentation for details:

- Edison HealthLink Site Installation Manual (MyWorkshop documents DOC2300779 (EHL 1.3), DOC2406370 (EHL 1.4) and DOC2445146 (EHL 1.5))
- Edison HealthLink Platform Service Guide (MyWorkshop documents DOC2300778 (EHL 1.3), DOC2406382 (EHL 1.4) and DOC2445143 (EHL 1.5))
- Smart Subscription 2.0 Service Manual 5867662-8EN
- CT Scanner Service Method
- This Service Manual.

Prerequisites:

- The Edison platform software is installed.
- For CT Console only: the CT option key [SmartSubscription -Connection] is installed.
- The Edison Admin Console is available with login and password.
- The USB media containing the combined OS and the AW Server qcow2 image template. Refer to [1.3 Software Kit on page 23](#).
- The USB media with Volume Viewer Application.
- One Ethernet cable to connect the FE laptop to the Edison private network.
- The FE laptop shall be able to connect to the Edison HealthLink using private network static IP 172.16.0.200. For full procedure description, refer to the Edison HealthLink Site Installation Manual, section Laptop Setup to static 172.16.0.200.

#### **NOTE**

In the below sections, when requested to use a USB media (for configuration or licenses file generation), always use a GE validated read/writeable USB media.

For an AW Server installation execute the following sections:

- Installation/Upgrade Preparation
- AW Server Installation
- Applications Installation/Upgrade
- AW Server final Settings
- AW Server feature connection - CT Console

For an AW Server upgrade execute the following sections:

- Installation/Upgrade Preparation
- AW Server Upgrade

#### **NOTE**

There are several types of upgrades (automatic, manual, Service Pack). In this section you are guided to the right sub-sections depending on the type of upgrade.

- Applications Installation/Upgrade
- AW Server final Settings
- AW Server feature connection - CT Console

All sections are performed and completed by the GEHC FE.

## 2.29.1 Installation/Upgrade Preparation

This section describes the steps to prepare the AW Server and/or Applications installation or upgrade within the Edison HealthLink.

### 2.29.1.1 AW Server files preparation

The AW Server software is delivered using two methods:

- [Physical Software Kit on page 23](#) (USB media was obtained from manufacturing or through parts):

Part Number	Content	Purpose
5818084-10  (or higher) 	<i>aws-3.2-4.9-0.qcow2.iso</i>	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.
	<i>startinstallwizard.bat</i> or <i>startinstallwizard.sh</i>	These scripts are used for <b>Initial Installation</b> to prepare the AW Server configuration (on Windows or on Linux).

#### NOTE

The reference checksum file (.sha256 extension) is not listed in the table. However, it is present in the USB media to verify file integrity.

- [Digital Software Kit on page 25](#) (eDelivery). Use the following files to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose
<i>5865570-5_AW_Server_3.2_Ext.4.9_and_OS_QCOW2_Template_for_VM.iso</i>	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.
<i>5865572-5_AW_Server_3.2_Ext.4.9_VM_Install_Wizard.zip</i>	This compressed package is used for <b>Initial Installation</b> to prepare the AW Server configuration.

#### NOTE

The reference checksums, to verify files integrity, are listed in the *packagemetadata.json* files.

#### NOTE

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

### 2.29.1.2 Opening a console/terminal on the Edison HealthLink

1. From the FE laptop, in a web browser (Firefox or Internet Explorer), type in the iLO IP address and login to the iLO.  
  
Check with IT team for iLO IP address, username and password.
2. Start the Java Web Start Console (console/terminal).
3. Login to the console/terminal using the Controller Default credential.

Refer to the Edison HealthLink Site Installation Manual, section iLO Console and Java Web Start Console.

## 2.29.2 AW Server Installation

This section describes the steps to install, deploy and configure the AW Server within the Edison HealthLink, from the USB media.

### 2.29.2.1 Getting the MAC address and the network information for the AW Server Virtual Machine

1. Login to Horizon OAM Titanium Cloud from a web browser with the URL `https://<OAM IP Address>`, using `edison-usr` credential:  
Refer to the [Horizon/OAM/Titanium Cloud Dashboard] section in the [Edison HealthLink Platform Service Guide] for login to OAM.
2. Select **Project > Network > Networks > um-net0 > Ports**.
3. Note the MAC address and the IP address.

Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
(075e4ecb)	192.168.103.2	fa:16:3e:e6:ee:88	network:dhcp	Active	UP	<button>Edit Port</button>
vrouter1_um_net0_port	192.168.103.254	fa:16:3e:d2:db:7b	network:router_interface	Active	UP	<button>Edit Port</button>
(b09015d4)	192.168.103.1	fa:16:3e:2ff:53	network:router_interface	Active	UP	<button>Edit Port</button>
aw_port	192.168.103.3	fa:16:3e:86:bf:39	compute:nova	Active	UP	<button>Edit Port</button>

4. In the **Subnets** tab, note the network prefix (in **Network Address**) and the **Gateway IP**.

Name	Network Address	IP Version	Gateway IP
um-subnet0	192.168.103.0/24	IPv4	192.168.103.1

### 2.29.2.2 Preparing the AW Server configuration with the Installation Wizard

Prepare the AW Server configuration using the Installation Wizard. The Installation Wizard allows preparing and performing the basic AW Server configuration. It generates a configuration file that can be interpreted by the AW Server to perform the configuration automatically during its first start (Cloud-init mechanism).

### 2.29.2.2.1 Launching the Installation Wizard

The Installation Wizard is present in the USB media.

1. Insert the AW Server USB media into an USB port of the laptop.
2. On the laptop, create a folder and name it AWS\_EXT4.9.
3. Copy the following file and folders from the USB media to the AWS\_EXT4.9 folder:

```
app  
jre  
startinstallwizard.bat
```

4. Remove the USB media from the laptop.
5. Navigate to the AWS\_EXT4.9 folder and double click on **startinstallwizard.bat** script.

The Installation Wizard appears.

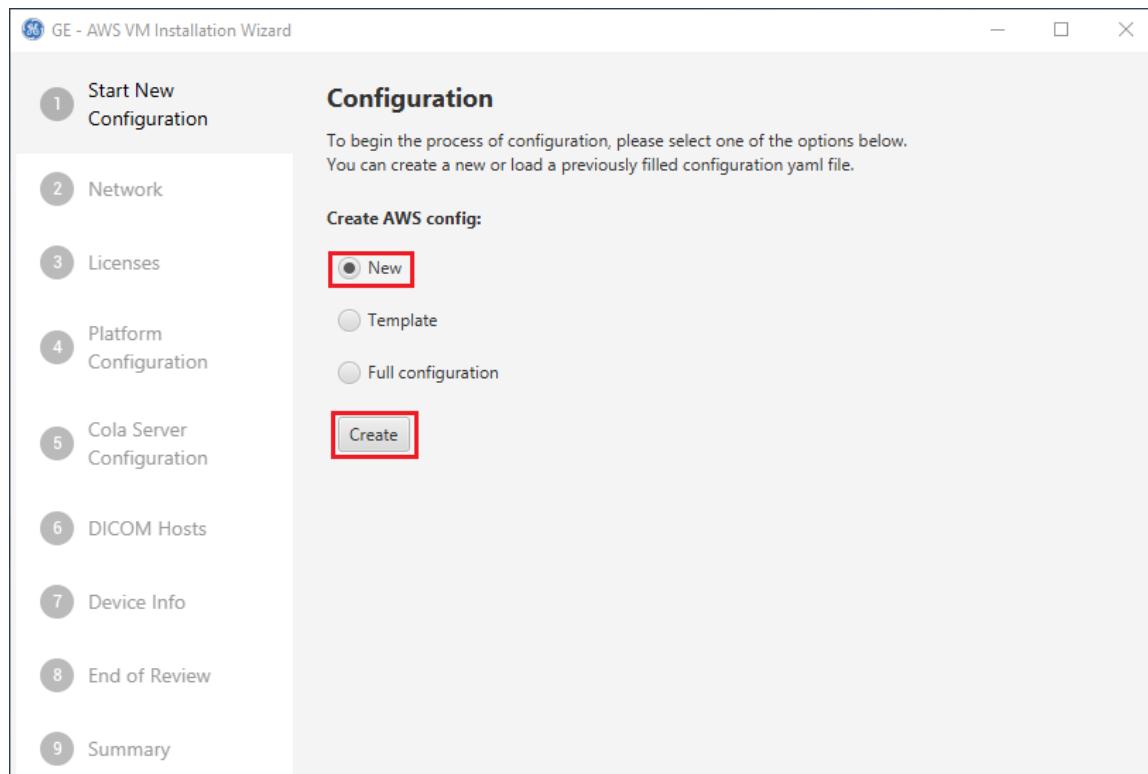
#### NOTE

The Installation Wizard can also be launched from the EHL system using the `startinstallwizard.sh` script after mounting the USB media. It is recommended to run it on the laptop so that the configuration file can be saved and re-used if necessary.

### 2.29.2.2.2 Starting the Installation Wizard configuration

To create a new configuration:

1. In the **Start New Configuration** tab, select **New**.
2. Click on **Create**.



### 2.29.2.2.3 Installation Wizard navigation and Field Filling Rules

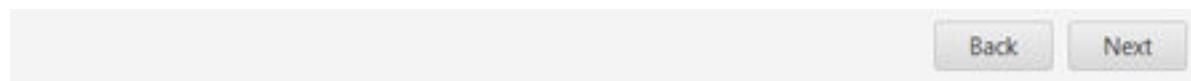
In the following steps all fields marked with an asterisk (\*) are mandatory and must be filled out. Other fields are optional.

If a field is wrongly filled, the symbol  appears next to the field and also on the corresponding tab and the *Summary* tab, as shown in the example below.

When all the mandatory fields are correctly filled, a green check appears near the fields and on the tab, as shown in the example below:

Set up network interfaces:	
Network	Licenses
Host name*: awsnano 	Domain name: 
IP*: 192.168.101.5 	Network prefix*: 24 
Field wrongly filled (here the IP field)	Field correctly filled

To navigate through the tabs click directly on the tab or on the **Next** and/or **Back** buttons at the bottom right of the Installation Wizard.



#### NOTE

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#), to know the characters rules and limitations of the specific fields (Hostname, AE Title, IP Address, Port, System ID, Label/Name).

#### 2.29.2.2.4 Configuring the network and time settings

- Get all network information noted in [2.29.2.1 Getting the MAC address and the network information for the AW Server Virtual Machine on page 310](#).
- In the **Network** tab, enter the **Host name**, the **IP address**, the **Network prefix**, the **Default Gateway** and the **MAC address**.

## Network Configuration

Please fill the information below about your VM's network and time settings.

Please note:

The MAC address shall be retrieved from the created VM.

Changing the MAC address will clear all the previously filled license information.

When adding multiple NTP Server the first one in the list will be used.

NTP server is case insensitive and it is mandatory when cluster mode is enabled.

### Set up network interfaces:

Host name*:	aws	✓
Domain name:		
IP*:	192.168.103.3	✓
Network prefix*:	24	✓
Gateway:	192.168.103.1	✓
DNS 1:		
DNS 2:		
MAC address*:	16:3e:86:bf:39:3e	✓

### Time settings:

Region:	Europe
City:	Paris
NTP server*:	<input type="text"/> Add

3. In the *Time settings* panel, select the **Region** and the **City**.
4. The **NTP server**'s IP address is not mandatory.
5. Click on **Next**.

### 2.29.2.2.5 Configuring the licensing settings

- In the **Licenses** tab, click on **Copy** to copy the license ID in the clipboard.

**Generate eLicenses**

Please generate the licenses from the e-license website, using the License ID.

MAC address of NIC 1: 00:50:56:8a:43:0a

License ID: 068a430a **Copy**

Copy the created License ID, then use this link to generate eLicenses: **Go to eLicense Site**

**Add eLicences**

License file: C:\Users\100005286\Downloads\config **Browse** Remove All

**Uploaded Licenses**

License Name	License Key
AutoBone_Xpress	ZU3C7MOCNJ7N9XS3
Volume_Viewer	3SU9AYMOXVBKNPYX

- Get the site System ID or GON (Global Order Number) listed on the site's paperwork from GEHC.
- Generate the eLicenses file:  
Refer to [A.3 Licensing on page 556](#) for the complete procedure.
  - Click on **Go to eLicense Site** to access the GEHC eLicense website.
  - Or access the GEHC eLicense website from <http://elicense.gehealthcare.com/elicense/> OR <http://elicense.gehealthcare.com/> - this URL is available via the Internet, and via the GEHC VPN connectivity model.

#### NOTE

If you can't connect to eLicense, contact the OLC and ask them to obtain the licensing information for you.

- Click on the **Browse** button and locate the eLicenses file generated in previous point and saved on your laptop.
- Select the eLicenses files then click on **Open** to load the file.  
The licenses appear in the *Upload Licenses* list.
- Click on **Next**.

### 2.29.2.2.6 Configuring the platform settings

In the **Platform Configuration** tab, the Platform Integration Mode is filled based on the imported eLicense file.

1. Select **DICOM Direct Connect** integration mode.
2. Enter the **Authentication URL**:
  - For a CT Console: **<http://172.16.0.1:9999/host>**
  - For an MR Console: the public IP address of the MR console.

## Platform Configuration

The Platform Configuration is automatically filled based on the imported license file.  
Please review and select the appropriate configuration and fill out the remaining information if needed.  
Note : Console Host IP address field is only for Nano licenses.

### Platform Integration Mode

<input type="radio"/> Standalone	<input checked="" type="radio"/> DICOM Direct Connect (PACSinteg plugin)
Platform enabler*:	SdC_Low_Tier_Premium
Platform license key*:	7FWBD8L83GBOES9D
Integration license key*:	3YYFB7D676DORRU6
Authentication URL:	<input type="text" value="http://172.16.0.1:9999/host"/>
Console host IP address*:	<input type="text"/>
Preprocessing license key (AutoLaunch):	Not set

3. Click on **Next**.

### 2.29.2.2.7 Configuring the license server(s) settings

In the **Cola Server Configuration** tab, the License Server configuration is automatically filled based on the imported eLicense file. No input is required.

## License Server Configuration (CoLa Server)

The License server configuration is automatically filled based on the imported license file.  
In case a Cola Server is not part of your license, you can manually fill the parameters and define external Cola Server. Please review the appropriate configuration.

Built-in

Server enabler: 2DBVD8NGPE8G8OV8

Primary license server IP\*:  ✓

Secondary license server IP:

Server port\*:  ✓

Click on **Next**.

## 2.29.2.2.8 Configuring DICOM hosts

In the **DICOM Hosts** tab, configure the CT/MR Console as a DICOM host:

1. Enter the CT/MR host name in the **Name, Host name** and **Application Entity Title** fields.

### DICOM host configuration:

Please fill the information below about your DICOM host configuration.  
Use the "Create host" button to create your DICOM Hosts and continue with the configuration.

#### Create new DICOM host:

Name*:	bay99	✓
Host name*:	bay99	✓
Application Entity Title*:	bay99	✓
IP address or domain name*	172.16.0.1	✓
Port*:	4006	✓
Query/retrieve supported:	<input checked="" type="checkbox"/>	
Custom search:	<input type="checkbox"/>	
Encrypted (TLS)	<input type="checkbox"/>	

► Request optional DICOM tags  
► Storage Commitment  
► PACS query retrieve options  
► Web Services link option and comments  
► DICOM Direct Connect settings

#### Created DICOM hosts:

bay99
-------

**Create host**

2. Enter the **IP address**:

- For a CT Console: the eth0 IP address of CT console.
- For an MR Console: the Public Floating IP of the console.

3. Check the **Port** is 4006.

4. Click on **Create host**.

The DICOM host appears in the **Created DICOM hosts** list.

Created DICOM hosts:
bay99

5. If needed, repeat all previous steps to create other DICOM hosts.

6. Click on **Next**.

### 2.29.2.2.9 Filling out the device information

- Enter the site information in the **Device Info** tab of the Installation Wizard, as shown in the example below:

**Device Information**

Add device information

AWS System ID/AWS CRM number*	<AWS_SYSTEMID>	✓
Contract number:		
Global order number*	TC06NAQAWS	✓
Install date*:	10/18/2022	<input type="button" value="Calendar"/> <input type="button" value="Delete"/>
Expiration date:		<input type="button" value="Calendar"/> <input type="button" value="Delete"/>
Device description:		
Hospital name*:	AWBUC ENG LAB	✓
Address (line 1)*:	BUC	✓
Address (line 2):		
City*:	BUC	✓
State:		
Postal code:		
Country:	FR, France	▼
Other country:		
Address description:		
Service area:		
Service processor IP address:		

- Fill in the **AWS System ID / AWS CRM number** field with the unique AW Server System ID.

**NOTE**

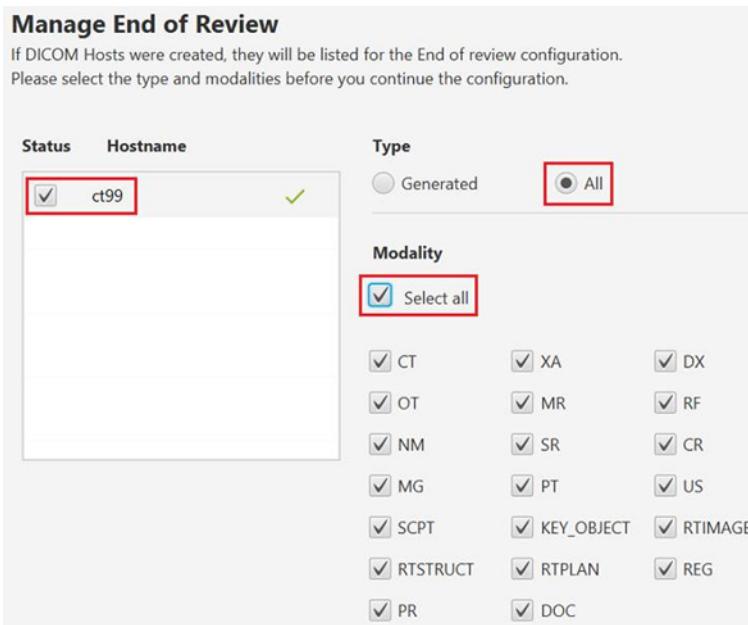
For the system connected via RSvP, the AW Server has a separate RSvP connection. As such, the AW Server has a unique System ID. The AW Server System ID has been created as part of the Edison HealthLink order. Refer to the project manager for any help on the AW Server System ID.

- Fill in the **Global order number**, the **Install date**, the **Hospital name**, the **Address (line 1)** and the **City** fields.
- Click on **Next**.

### 2.29.2.2.10 Configuring End of Review

The End of Review feature automatically sends processed images to the CT Console (configured as a DICOM Host), or to any other DICOM host, when exiting the application.

1. In the **End of Review** tab, check the checkbox under the **Status Hostname** area to enable the End of Review process.



2. In the *Type* panel, select **All**.
3. In the *Modality* panel, check **Select all**.
4. Click on **Next**.

### 2.29.2.2.11 Saving the configuration

1. In the **Summary** tab, review the configuration.

Use the scroll bar to review the settings from the previous sections.

**Configuration Summary**

Please review all the configuration information you can modify the parameters by going back to the appropriate page.  
To export the configuration, please select one export option from the list according to your deployment mode.  
After export you can start a new configuration or exit the application.

**Network Configuration**

Host name:	aws
Domain name:	Not filled
IP:	192.168.103.3
Network prefix:	24
Gateway:	192.168.103.1
DNS 1:	Not filled
DNS 2:	Not filled
MAC address:	16:3e:86:bf:39:3e
Time zone (Region/City):	Europe/Paris
NTP servers:	Not filled

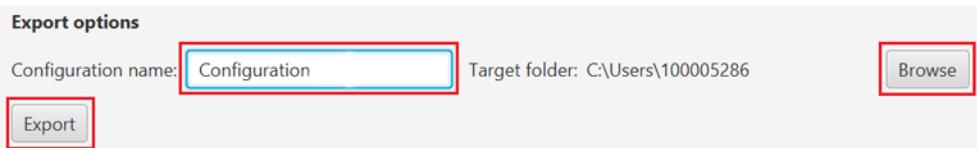
**eLicenses**

License ID:	sahf2020
-------------	----------

2. Click on **Browse** to choose the location where you want to save the Configuration folder.

- Click on **Export**, the Configuration folder will be created in the location you previously choose.

The Configuration folder contains the user-data and YAML files.



A pop-up appears.

- Click on **Exit** to save the configuration and exit the Install Wizard.

The Configuration.yaml and user-data files are created in the Configuration folder. Ignore the other files present.

- Copy the configuration folder to an USB media.

### 2.29.2.3 Deploying the AW Server on a Virtual Machine

- Insert the USB media with the configuration folder into the Edison HealthLink.
- Identify the USB media by typing the following command in the console/terminal of the Edison HealthLink:

```
sudo fdisk -l <Enter>
```

#### NOTE

The first time you use **sudo** command you may have to enter the **wrsroot** password.

The last USB media inserted will be **displayed as the last item** within the **Device Boot** section, in the output of the command.

```
Disk /dev/sdaa: 64.2 GB, 64160400896 bytes, 125313283 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xe637597e

      Device Boot      Start        End      Blocks   Id  System
/dev/sdaa1            128    125313250   62656561+   7  HPFS/NTFS/exFAT
controller-0:~$
```

Or, if the **Device Boot** section is empty, the USB media will be **displayed as the last Disk**.

```
Disk /dev/sdc: 32.2 GB, 32212254720 bytes, 62914560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x00000000

      Device Boot      Start        End      Blocks   Id  System
controller-0:/opt/backups$
```

Record the USB media name (here /dev/sdc), as it will be used in below commands.

- Navigate to the /opt/backups directory:

```
cd /opt/backups <Enter>
```

4. Mount the USB media using the following commands:

```
sudo mkdir -p mnt/awserver_package <Enter>
sudo mount /dev/sdc mnt/awserver_package <Enter>
```

**NOTE**

Here we assume that the USB partition is /dev/sdc. If it is not the case, replace /dev/sdc by the right USB partition as identified in [Step 2](#).

5. Remove the ees/awserver directory if any and (re)create it:

```
sudo rm -rf ees/awserver <Enter>
sudo mkdir -p ees/awserver <Enter>
```

6. Copy the yaml file and the user-data file using the following commands:

```
sudo cp -f mnt/awserver_package/Configuration/*.yaml ees/awserver
<Enter>
sudo cp -f mnt/awserver_package/Configuration/user-data ees/awserver
<Enter>
```

7. Unmount the USB partition:

```
sudo umount mnt/awserver_package <Enter>
```

8. Remove the USB media from the Edison HealthLink.

9. Insert the USB media with the preinstalled OS and AW Server into the Edison HealthLink.

10. For versions EHL 1.5.2 and older, mount the USB media in read-only using the following command:

```
sudo mkdir -p mnt/usb_img <Enter>
sudo mount /dev/sdc mnt/usb_img <Enter>
```

**NOTE**

Here we assume that the USB partition is /dev/sdc. If it is not the case, replace /dev/sdc by the right USB partition as identified in [Step 2](#).

```
sudo mount -ro loop mnt/usb_img/aws-3.2-4.9-0.qcow2.iso \
mnt/awserver_package <Enter>
```

**NOTE**

The qcow2.iso file name used here, is the one from the Physical Software Kit. So, it is different if using a Digital Software Kit.

11. Create the Virtual Machine, deploy the AW Server and automatically configure the AW Server using the following command:

For versions EHL 1.5.2 and older:

```
edison vm -install /opt/backups/mnt/awserver_package <Enter>
```

From version EHL 1.5.3:

```
edison vm install <Enter>
```

Wait for the message "VM Installation successfully completed....." to display (roughly 5mn).

```

aw-server-0-volume-os Stack CREATE started
aw-server-0-volume-os Stack CREATE completed successfully
aw-server-aw.low_tier_premium-0 Stack CREATE started
aw-server-aw.low_tier_premium-0 Stack CREATE completed successfully
VM Installation successfully completed.....
controller-0:~$ [1012436.982885] kvm [5122]: vcpu0 unhandled rdmsr: 0x345

```

Press <Enter> to return to prompt.

- For versions EHL 1.5.2 and older, unmount the USB partition:

```

sudo umount mnt/awserver_package <Enter>
sudo umount mnt/usb_img <Enter>
cd <Enter>

```

- Remove the USB media from the Edison HealthLink:

Ignore the error message when removing the USB media.

Press <Enter> to return to prompt.

This completes the Virtual Machine creation with the AW Server deployment and the AW Server configuration.

## 2.29.2.4 Displaying the AW Server Console

The below steps described the process to display the AW Server Console from the Edison HealthLink.

### NOTE

Refer to the *Edison HealthLink Platform Service Guide*, section *Horizon/OAM/Titanium Cloud Dashboard*.

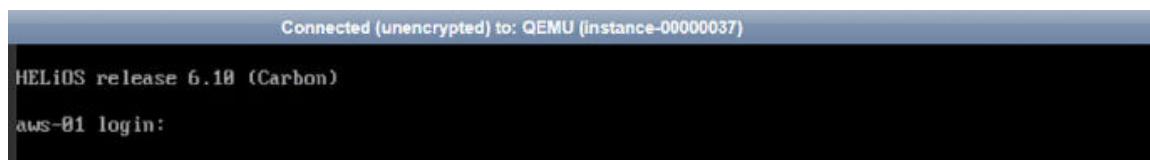
- Login to Horizon OAM Titanium Cloud from a Web Browser with the URL: <https://<OAM IP Address>>, using **edison-usr** credential.
- Select **Project > Compute > Instances**.
- Click on **aw-server-0** in **Instance Name**.

Instance ID	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
	aw-server-0	(not found)	192.168.103.3	aw-low-tier-premium	aw-keypair	Active	az1	nova	NONE	Running	1 week, 1 day	<a href="#">Create Snapshot</a>
	cp-galana-0	es-cantos7	192.168.101.18	mt.small	cd-keypair	Active	az1	nova	NONE	Running	3 weeks	<a href="#">Create Snapshot</a>

4. In the **Console** tab, click on **Click here to show only console**.



The AW Server Console appears:



5. If the AW Server Console does not appear and the error message 503 Service Unavailable appears:

- a. In the console/terminal of the Edison HealthLink, type:

```
cd /home/wrsroot/tic_support <Enter>
sudo ./vnc_service_tool.sh <Enter>
```

The following message appears:

```
System is operational and enabled.
1) Enable_VNC_Console
2) Disable_VNC_Console
3) Quit
Please enter your number choice:
```

- b. Type:

```
1 <Enter>
```

The following message appears:

```
Removing security rule.
+-----+-----+
| Property      | Value
+-----+-----+
| uuid          | db26b919-4fe4-4544-9d0e-41e8745aa63f |
| firewall_sig  | 67ad602b11caf988a8d1cae14340ce01   |
| updated_at    | 2020-08-26 18:09:07.053625+00:00   |
+-----+-----+
checking for multiple rules...
security rules cleared...
VNC will remain enabled only for 3 hours.
```

## 2.29.2.5 Configuring the HA Proxy for AW Server

In order to be able to access the AW Server through the Edison HealthLink, the HA Proxy shall be configured to forward the ports needed by the AW Server.

Refer to the Edison HealthLink Site Installation Manual, section Application Software Installation, subsection For AW Server.

1. To configure the HA Proxy for AW Server, in the console/terminal of the Edison HealthLink, type the following commands:

```
cd /home/wrsroot/kindler/site_utils <Enter>
sudo ./haproxy_update.py awserver <Enter>
```

### NOTE

In some Edison HealthLink version the `site_utils` folder may not exist and the command may have another extension. In this case type the following commands instead:

```
cd /home/wrsroot/kindler/shell_scripts <Enter>
sudo sh haproxy_update.sh awserver <Enter>
```

## 2.29.2.6 Updating static routing file on AW Server

### NOTE

This section is not applicable for the [MR Smart Subscription on Edison HealthLink](#).

1. In the AW Server console, login as `root`.

### NOTE

To display the AW Server Console, refer to [2.29.3.5.3 Displaying the AW Server Console on page 344](#).

2. Create the file `route-static-eth0` with the following text, as follow:

```
echo "172.16.0.0/24 via 192.168.103.254 dev eth0" >> /etc/sysconfig/
network-scripts/route-static-eth0 <Enter>
```

3. Restart the network service by typing the following command:

```
service network restart <Enter>
```

4. Confirm that the `172.16.0.0` has been added to the destination by typing the following command:

```
route <Enter>
```

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.103.0	*	255.255.255.0	U	0	0	0	eth0
172.16.0.0	host-192-168-10	255.255.255.0	UG	0	0	0	eth0
link-local	*	255.255.0.0	U	1002	0	0	eth0
default	host-192-168-10	0.0.0.0	UG	0	0	0	eth0

5. Confirm that ping connectivity is successful by typing the following command:

```
ping 172.16.0.1 <Enter>
```

```
[root@aws-08 network-scripts]# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=63 time=1.31 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=63 time=0.172 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=63 time=0.177 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=63 time=0.194 ms
^C
--- 172.16.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3798ms
rtt min/avg/max/mdev = 0.172/0.465/1.318/0.492 ms
[root@aws-08 network-scripts]# _
```

- To make the changes effective, type the following command:

**/etc/sysconfig/network-scripts/ifup-routes static -eth0 <Enter>**

- Return to login mode by typing the following command:

**exit <Enter>**

## 2.29.2.7 Allocating floating IP address for AW Server

Allocate floating public IP address for the AW Server.

### NOTE

Refer to the *Edison HealthLink Platform Service Guide*, section *Horizon/OAM/Titanium Cloud Dashboard*.

- Get the two Server IP addresses of the Edison HealthLink:

- Login to Horizon OAM Titanium Cloud from a Web Browser with the URL: <https://<OAM IP Address>>, using **edison-usr** credential.
- Select **Project > Network > Floating IPs**.

IP Address	Mapped Fixed IP Address	Pool	Status	Actions
172.16.0.120	-	external-net1	Active	<b>Disassociate</b>
10.135.248.25	-	external-net0	Active	<b>Disassociate</b>

- Record the following two IP Addresses:

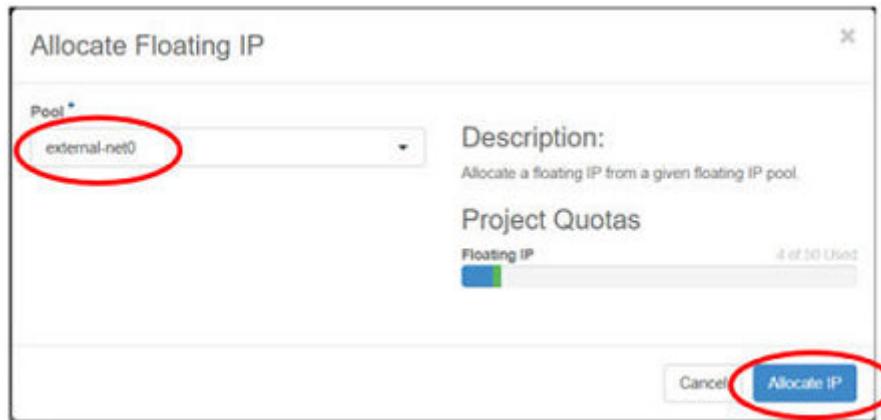
- Edison proxy floating IP (external-net0): \_\_\_\_\_
- Edison private proxy floating IP (external-net1): \_\_\_\_\_

Refer to the *Edison HealthLink Platform Service Guide*, section *Verify Edison IP Address*.

- Allocate Floating IP Address (Public) for AW Server:

- Click on **Allocate IP To Project**.

- b. The following window displays:



Select **external-net0** and click on **Allocate IP** to proceed.

After a few seconds, the new public IP address is added to the Floating IPs list.

Record the added New Public IP Address number.

- c. Move to **Project > Compute > Instances**.  
d. For **aw-server-0** instance, select **Associate Floating IP** in the pull-down menu.

The screenshot shows the 'Instances' page in the WIND interface. The left sidebar is collapsed. The main area shows a table of instances. One row for 'aw-server-0' is highlighted with a red box. To the right of the table, there are several actions: 'Create Snapshot', 'Associate Floating IP' (which is also highlighted with a red box), 'Edit Instance', and 'Attach Volume'. The 'Associate Floating IP' button is located at the bottom right of the actions panel.

- e. Select the previously recorded IP Address in the pull down menu and click on **Associate**.

The screenshot shows the 'Manage Floating IP Associations' dialog box. It has two input fields: 'IP Address \*' containing '10.135.248.24' and 'Port to be associated \*' containing 'aw-server-0: 192.168.103.3'. A descriptive text on the right says 'Select the IP address you wish to associate with the selected instance or port.' At the bottom are 'Cancel' and 'Associate' buttons, with 'Associate' being highlighted by a red circle.

- f. Check that the new allocated Floating IP is added on the **aw-server-0**:

The screenshot shows the WIND Titanium Cloud interface. The left sidebar has 'Project' selected under 'Compute'. The main area is titled 'Instances' and shows a table with one row for 'aw-server-0'. The table columns are 'Instance Name', 'Image Name', 'IP Address', 'Flavor', 'Key Pair', and 'Status'. The 'IP Address' column contains two values: 'um-net0' and '192.168.103.3 10.135.248.24'. The last two digits of the floating IP are highlighted with a red box.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status
aw-server-0	(not found)	um-net0 192.168.103.3 10.135.248.24	aw.low_tier_premium	aw-keypair	Active

- g. Move to **Project > Network > Floating IPs**.

Confirm that the new allocated Floating IP address for AW Server is added at the **aw-server-0**:

The screenshot shows the WIND Titanium Cloud interface. The left sidebar has 'Network' selected under 'Compute'. The main area is titled 'Floating IPs' and shows a table with four items. The table columns are 'IP Address', 'Mapped Fixed IP Address', 'Pool', and 'Status'. The 'IP Address' column contains '172.16.0.120', '10.135.248.25', and '10.135.248.24'. The last item, '10.135.248.24', is associated with 'aw-server-0 192.168.103.3' in the 'Mapped Fixed IP Address' column. This row is highlighted with a red box.

IP Address	Mapped Fixed IP Address	Pool	Status
172.16.0.120	-	external-net1	Active
10.135.248.25	-	external-net0	Active
10.135.248.24	aw-server-0 192.168.103.3	external-net0	Active

## 2.29.2.8 Reviewing the network settings

- In the AW Server console, login as **root**.

To display the AW Server Console, refer to [2.29.2.4 Displaying the AW Server Console on page 321](#).

- In the console type the following command to see the ethernet interfaces:

**ip addr <Enter>**

Check that for eth0:

- The MAC Address (link/ether) is assigned (not blank).
- The IP address (inet) is the same as the **aw-server-0** IP address.

```
[root@aws ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:25:de:fc brd ff:ff:ff:ff:ff:ff
    inet 192.168.103.3/24 brd 192.168.103.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe25:defc/64 scope link
        valid_lft forever preferred_lft forever
3: dummy0: <NOARP,BROADCAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 1e:7f:61:df:e3:7f brd ff:ff:ff:ff:ff:ff
    inet 169.254.100.1/24 brd 169.254.100.255 scope global dummy0
        valid_lft forever preferred_lft forever
    inet6 fe80::1c7f:61ff:fedf:e37f/64 scope link
        valid_lft forever preferred_lft forever
[root@aws ~]#
```

**NOTE**

For any additional details on Network Settings, please refer to [2.13 Job Card IST005 - Network and Time Configuration on page 127](#).

## 2.29.2.9 Configuring the AW Server

This section describes the configuration needed for the AW Server within the Edison HealthLink.

**NOTE**

As the AW Server has been configured using the Installation Wizard (Cloud-init mechanism), The AW Server has been mostly configured. Follow the below sections to complete the configuration.

### 2.29.2.9.1 Launching Service Tools

The Service Tools allows to configure the AW Server.

1. Start the Services Tools from the FE laptop or the CT Console as follow:

- a. At the FE Laptop, open any Web Browser and type in:

**https://<new allocated Floating IP for AW Server><Enter>**

For instance: **https://10.135.248.24**

Or

**https://<Edison Proxy Floating IP>:5443<Enter>**

For instance: **https://10.135.248.25:5443**

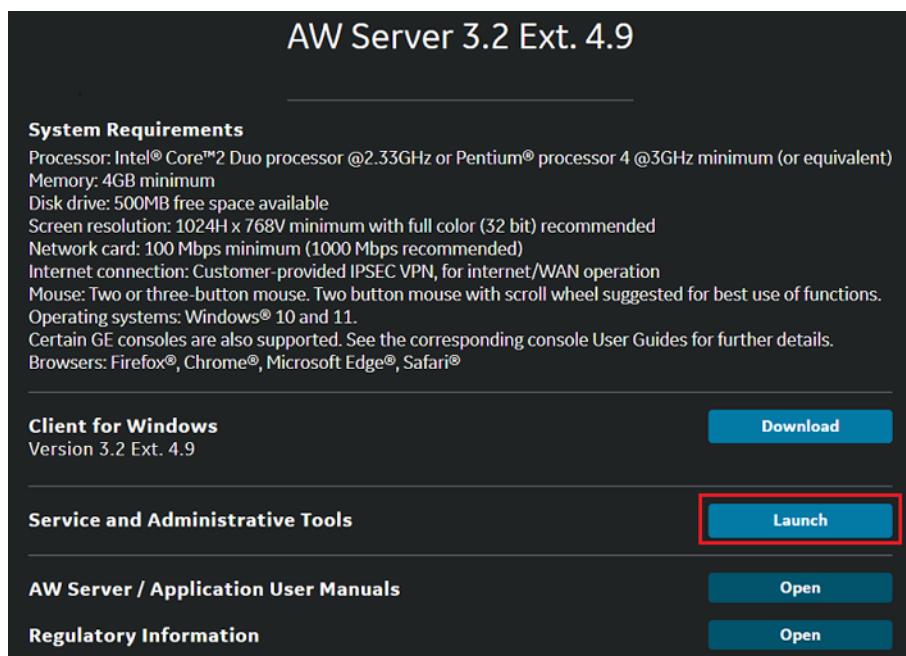
- b. At the CT Console, open any Web Browser and type in:

**https://<Edison Private Proxy Floating IP>:5443<Enter>**

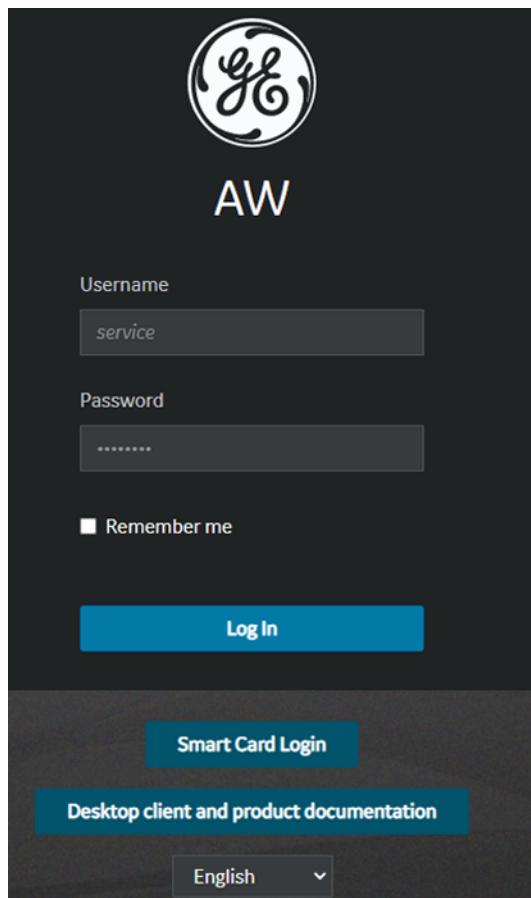
For instance: **https://172.16.0.120:5443**

2. Accept the cookies in the window that popups.

3. Click on the **Launch** button next to Service and Administrative Tools.



4. The login screen appears.



5. Login as **service**.

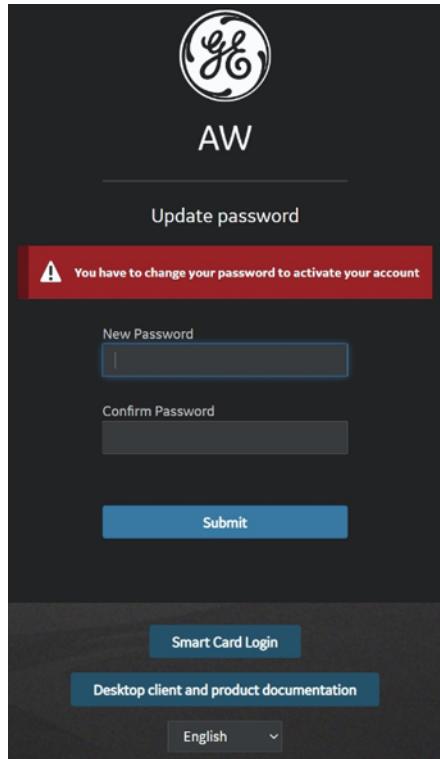
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

## NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for the password change guidelines.

6. The Service Tools opens with the installation/setup menus on the left.

 A screenshot of the Service Tools - AW Server interface. On the left is a sidebar with a search bar and links to 'HealthPage', 'Initial configuration', 'Administrative', 'Maintenance', 'Diagnostic', 'Tools', and 'Documentation'. The main area has a title 'Maintenance is in progress' with a timestamp 'since Oct 17, 2022, 2:28:33 PM'. It lists several tasks: 'Global Installed Base data is not sent yet to GE!', 'New package is available. [Click here for details](#)', 'Remote Service (RSvP) is not properly configured or not running. [Click here for details](#)', 'Last password generation and synchronization failed on Oct 30, 2022, 2:00:01 AM [Click here for details](#)', and 'Change all default passwords after installation!'. Below this is a 'HealthPage' section with a table of system status:
 

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

 There are also 'Status Details' and 'Refresh' buttons. At the bottom is a 'System Configuration' table:
 

System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.29.2.9.2 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, as shown below.

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.

**NOTE**

**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

### 2.29.2.9.3 Setting up Remote Service

The below sections describe how to configure the AW Server for Remote Connectivity (GEHC only).

**NOTE**

For information, the RSvP model type for AW Server 3.2 is: AWS32\_RSVP.

**NOTE**

The AW Server has a separate RSvP connection. As such, the AW Server has a unique **System ID (CRM Number)** which has been created as part of the Edison HealthLink order. Refer to the project manager for any help on the AW Server System ID

### 2.29.2.9.3.1 RSvP Remote Service Setup

- From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration.**

The **Configure RSvP Agent** panel displays.

The screenshot shows the 'Configure RSvP Agent' interface with three main sections: Overview, Settings, and Features.

**Overview:**

Agent	Status
Running	No
Connected	Unknown
Registered	Unknown
CRM Verified	Unknown
Quarantine	Unknown
Connection time	Unknown

**Settings:**

Agent	Configuration
System ID (CRM Number) *	<AWS_SYSTEMID>
Serial Number *	<Mandatory>
Display Name	
Model Number *	AWS32_RSVP
Version	2.3

Enterprise Server	Configuration
Hostname / IP *	insite.gehealthcare.com
Port Number *	443

Proxy Server	Configuration
Hostname / IP	
Port Number	

\* Mandatory fields

**Features:**

Feature	Status
Prodiags	Enabled

2. Select the **Settings** tab.

Agent		Configuration
System ID (CRM Number) *	<AWS_SYSTEMID>	
Display Name		

Enterprise Server		Configuration
Name	Production	
Hostname / IP *	insite.gehealthcare.com	
Port Number *	443	

Proxy Server		Configuration
Hostname / IP	PITC-Zscaler-EMEA-Amster	
Port Number	80	
Username	*****	
Password	*****	

\* Mandatory fields

3. In the **Agent** table, the **System ID (CRM NUMBER)** has been configured using the Installation Wizard (Cloud-init mechanism), check if the value is correct.

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.

4. In the **Enterprise Server** table, enter the **Name** of the RSvP server.

**NOTE**

There are two Enterprise Server, one in the US (e.g.: **Production**) and one in EU (e.g.: **Production-EU**). Use the one which is close to your location.

5. In the **Proxy Server** table, if the customer use a Proxy:

- Enter the **Hostname / IP** of the Proxy server.
- Enter the **Port Number** of the Proxy server.
- Enter the **Username** and **Password** of the Proxy server.

**NOTE**

This information can be acquired from the customer IT admin.

6. Click on **Save** button to save the RSvP settings.

**NOTE**

Use the **Refresh** button to reset the settings to the previous values entered.

Use the **Restart** button to restart the RSvP Agent.

7. In the **Overview** tab, review the RSvP settings.

<b>Agent</b>		<b>Configuration</b>
System ID (CRM Number) *		<AWS_SYSTEMID>
Serial Number *		AWBUCLAB243_20210201_183831
Display Name		AWBUCLAB243-Test
Model Number *		AWS32_RSVP
Version		2.3
<b>Enterprise Server</b>		<b>Configuration</b>
Hostname / IP *		insite-eu.gehealthcare.com
Port Number *		443
<b>Proxy Server</b>		<b>Configuration</b>
Hostname / IP		PITC-Zscaler-EMEA-Amsterdam3PR.proxy.corporate.ge.com
Port Number		80

\* Mandatory fields

8. Click on **Start** button to start the RSvP Agent.

The **Running** status turns green.

<b>Agent</b>	<b>Status</b>
Running	Yes
Connected	No
Registered	No
CRM Verified	No
Quarantine	Yes
Connection time	N/A

#### NOTE

Use the **Stop** button to stop the RSvP Agent.

Use the **Restart** button to restart the RSvP Agent.

9. Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green (except for the **CRM Verified** status - see [2.29.2.9.3.2 System ID \(CRM Number\) verification on page 334](#)).

#### NOTE

Do not hesitate to select the **Refresh** button again till the status turns green (see below status definition and latency to turn green).

<b>Agent</b>	<b>Status</b>
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	No
Quarantine	No
Connection time	Mon 1 Feb 2021 06:43:30 PM GMT+1

Status definition:

- **Running:** Value is **Yes** if the Agent is running. Otherwise, the value is **No**.
- **Connected:** Value is **Yes** if the Agent can be registered to the back office and is actively polling the back office. If the Agent is unable to successfully poll the back office, the value is **No**.
- **Registered:** Value is **Yes** if the Agent has successfully registered with the back office and has received confirmation of this registration. Otherwise, the value is **No**.

This value does not reflect if the Agent is actively polling. It is a 1 time notification of successful registration.

To see if the Agent is currently communicating with back office, see the **Connected** status.

#### **NOTE**

The **Yes** status may take a minute or two to appear.

- **CRM Verified:** If the value is **Yes**, it means that the System ID (a.k.a. CRM Number) is in CRM systems. Otherwise, the value is **No** (see [2.29.2.9.3.2 System ID \(CRM Number\) verification on page 334](#)).

#### **NOTE**

The **Yes** status may take up to 5 minutes to appear.

- **Quarantine:** Value is **Yes** if the Agent is currently in Quarantine. Otherwise, the value is **No**. If Agent status returns quarantine values as **Yes**, it means that RSvP back office cannot uniquely identify the device as some other device is also running an agent using the same System ID (CRM Number).

#### **NOTE**

The FE shall contact the RSvP team to resolve the issue.

- **Connection time:** Value is the last successful connection date/time of the RSvP Agent with the back office.

#### **NOTE**

The RSvP status is also displayed in the **Remote Service** table of the Healthpage.

## **2.29.2.9.3.2 System ID (CRM Number) verification**

#### **NOTICE**

It is important to have the System ID (CRM Number) verified now, so that the system will be able to upload its configuration to the AWCCT website and automatically receive in return the Registration Configuration key, necessary to enable the AW Server.

#### **NOTE**

Registration will have to be done manually if RSvP is not available.

#### **NOTE**

Without the Registration key, the AW Server will not allow exiting from the Maintenance mode and therefore be accessible to the Clients.

1. From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration**, check that the status of the RSvP Agent are green.

Agent	Status
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	Yes
Quarantine	No
Connection time	Mon 1 Feb 2021 07:46:44 PM GMT+1

2. If the **CRM Verified** status remains red, select the **Refresh** button to refresh the RSvP Agent status.

As mentioned in previous section, the **CRM Verified** status takes time to turn green.

If it remains red after 5 minutes, contact the local RSvP team to get the System ID (CRM Number) verified for the system.

When all the RSvP Agent status are green, the system is ready to be accessed remotely.

3. Proceed to the connection tests with FFA, to make sure the system is ready to be accessed remotely.

## 2.29.3 AW Server Upgrade

This section describes the steps to upgrade the AW Server within the Edison HealthLink.

There are 3 types of upgrades (automatic, manual, Service Pack). The automatic upgrade is not available in this version of the AW Server version within the Edison HealthLink.

- AW Server manual upgrade:

To upgrade the OS and AW Server Platform software (Load From Cold), execute the following sections:

- Launching Service Tools
- Navigating in Service Tools
- Entering the Maintenance Mode
- Backing up the configuration
- Manual OS and AW Server Platform software upgrade
- Restoring the saved configuration
- Restoring the integration
- Restarting the RSvP Agent

- AW Server Service Pack:

To install an AW Server Service Pack, execute the following sections:

- Launching Service Tools
- Navigating in Service Tools
- Entering the Maintenance Mode
- Backing up the configuration
- OS and AW Server Platform software Service Pack installation

### 2.29.3.1 Launching Service Tools

The Service Tools allows to configure the AW Server.

1. Start the Services Tools from the FE laptop or the CT Console as follow:

- a. At the FE Laptop, open any Web Browser and type in:

**`https://<new allocated Floating IP for AW Server><Enter>`**

For instance: **`https://10.135.248.24`**

**Or**

**`https://<Edison Proxy Floating IP>:5443<Enter>`**

For instance: **`https://10.135.248.25:5443`**

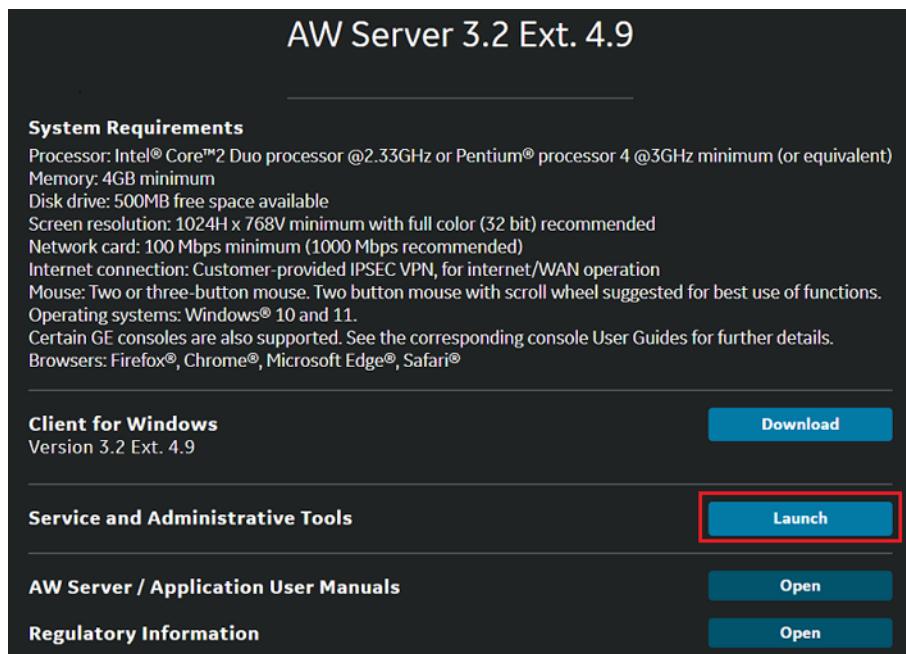
- b. At the CT Console, open any Web Browser and type in:

**`https://<Edison Private Proxy Floating IP>:5443<Enter>`**

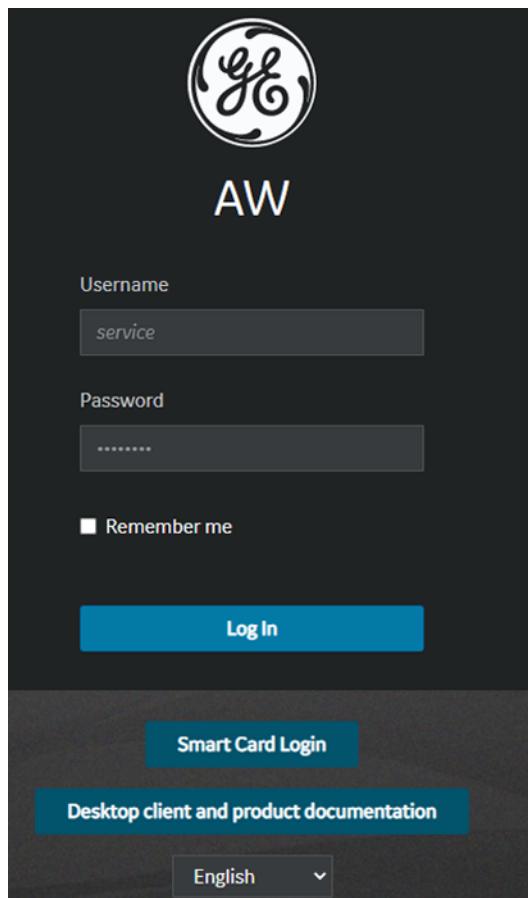
For instance: **`https://172.16.0.120:5443`**

2. Accept the cookies in the window that popups.

3. Click on the **Launch** button next to Service and Administrative Tools.



4. The login screen appears.



5. Login as **service**.

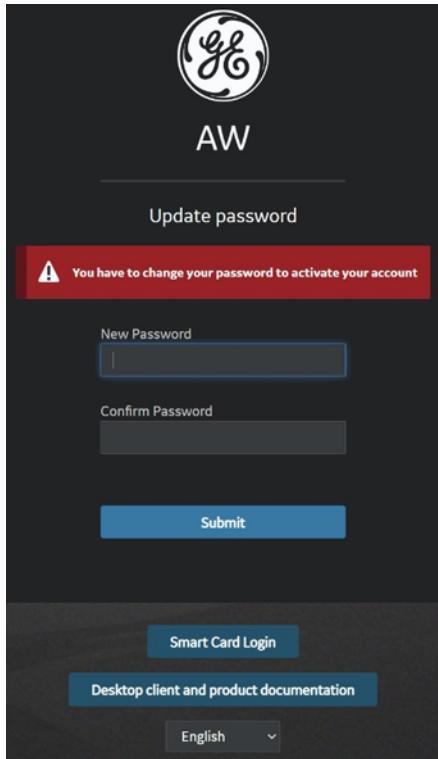
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

## NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.21 Job Card IST006 - Changing the Passwords](#) on page 249 for the password change guidelines.

6. The Service Tools opens with the installation/setup menus on the left.

 A screenshot of the Service Tools - AW Server interface. On the left is a sidebar with a search bar and links for 'HealthPage', 'Initial configuration', 'Administrative', 'Maintenance', 'Diagnostic', 'Tools', and 'Documentation'. The main area shows a 'Maintenance is in progress' message from Oct 17, 2022, 2:28:33 PM, listing tasks like 'Global Installed Base data is not sent yet to GE!' and 'Remote Service (RSvP) is not properly configured or not running'. Below this is a 'HealthPage' section with a table of system components and their statuses (CPU, Memory, Network Interface Controller, Storage, all OK), and a 'System Configuration' table with entries for System ID, Platform version, and Hostname/IP Address.
 

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

System Configuration	
System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.29.3.2 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, as shown below.

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.

**NOTE**

**Diagnostic** and **Tools** are not used for installation/setup.

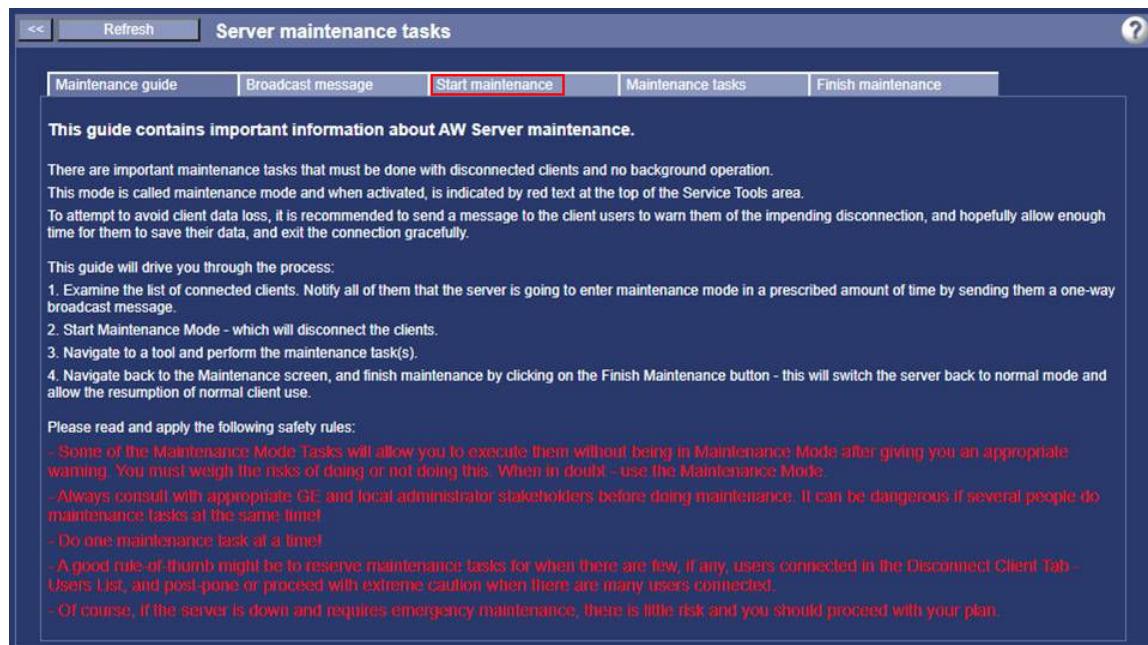
**Administrative > Utilities** is not used for installation/setup.

### 2.29.3.3 Entering the Maintenance Mode

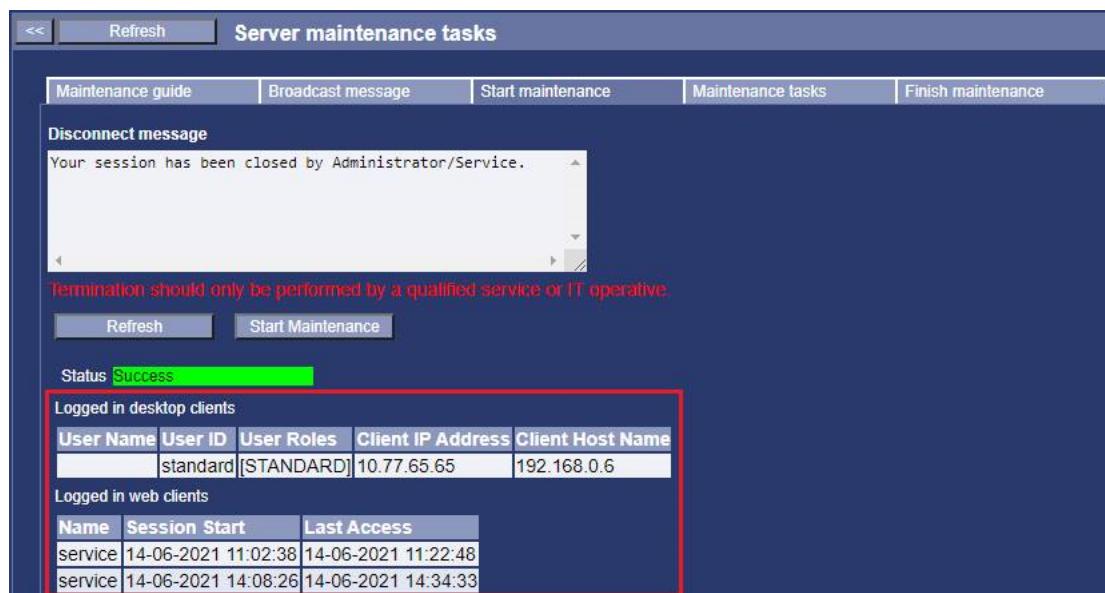
The Maintenance Mode allows the AW Server to be "isolated" from the AW Server Clients in order to perform maintenance operations such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters ...

Follow the below steps to place the AW Server in Maintenance Mode:

- From the Service Tools, select **Maintenance > Maintenance** and select the **Start maintenance** tab.

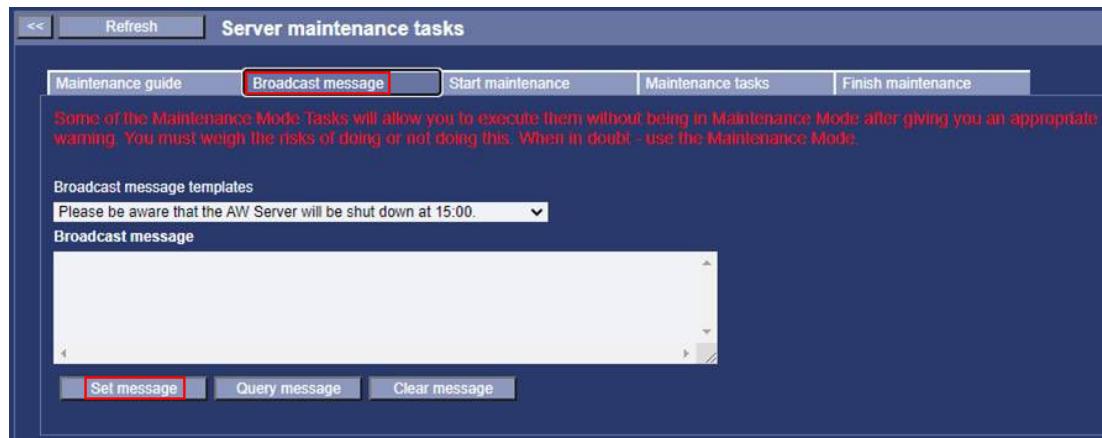


- If users are connected, they appear as in the page:



- If users are connected, send a broadcast message to the users:

- Select the **Broadcast message** tab.



- Write a message or modify the default message to adapt it to your needs. An example of broadcast message could be: "AW Server will be shutdown in 5 minutes, save your work before exiting."
- Click on **Set message** to broadcast it.

#### NOTE

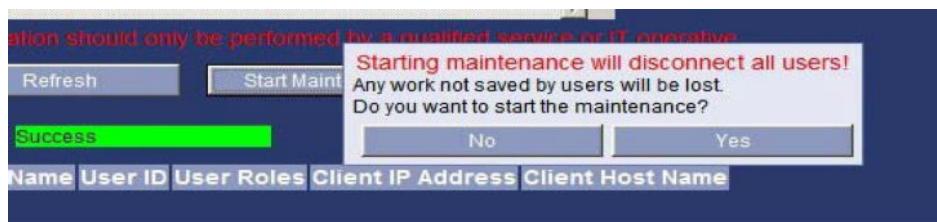
The **Query Message** button displays the last message entered. The **Clear Message** deletes all text in the message box. Always click **Clear Message** when done so that the last message is not inadvertently re-sent..

#### NOTICE

Allow a grace delay (a few minutes) for the users to save their work before disconnecting them by entering the Maintenance Mode.

- When the warning time has expired, come back to the **Start maintenance** tab and click on the **Start Maintenance** button to start the Maintenance Mode.

A pop-up confirmation message appears.



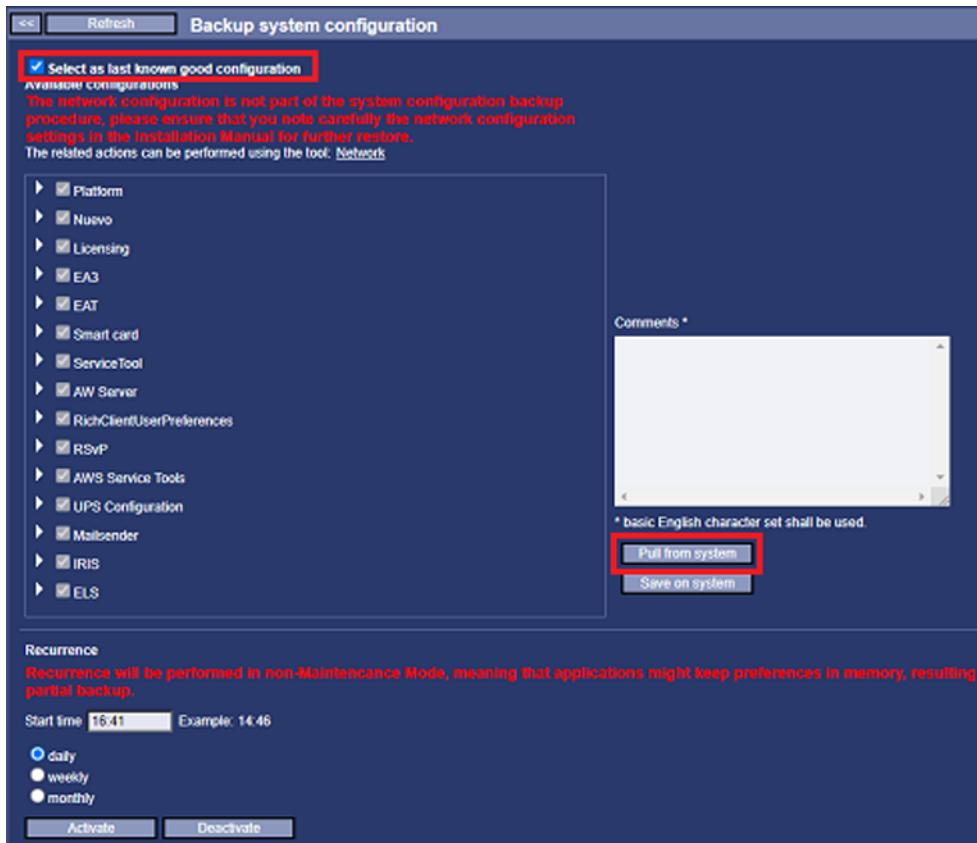
- Click on **Yes**.

Another pop-up states that you are in maintenance mode. And the Maintenance is in progress banner will display at the top of the Service Tools.



## 2.29.3.4 Backing up the configuration

- From the Service Tools, select **Maintenance > Backup > System configuration**.



- Check the **Select as last known good configuration** radio button.
- Keep everything selected and click on **Pull from system** to save the configuration on the local system.
- Copy the saved configuration on an USB media and keep it in a safe place.

## 2.29.3.5 Manual OS and AW Server Platform software upgrade

This section describes the upgrade/update of the AW Server (Load from Cold) integrated within the Edison HealthLink, from the USB media.

### 2.29.3.5.1 Deleting the AW Server instance from the Edison HealthLink

#### NOTE

Refer to the *Edison HealthLink Platform Service Guide*, section *Horizon/OAM/Titanium Cloud Dashboard*.

- Login to Horizon OAM Titanium Cloud from a Web Browser with the URL: `https://<OAM IP Address>`, using `edison-usr` credential.
- Select **Project > Compute > Instances**.

- For **aw-server-0** instance, select **Dissociate Floating IP** in the pull-down menu.

The screenshot shows the Horizon OAM Titanium Cloud interface under the Project > Compute > Instances section. A table lists several instances, including 'aw-server-0' which is highlighted with a red box. The 'Actions' column for 'aw-server-0' contains a dropdown menu with the option 'Disassociate Floating IP' highlighted by a red box.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
um-net0	(not found)	192.168.103.3 10.135.248.24	aw_low_tier_premium	aw-keypair	Active	fl-1 nova	None	Running	3 days, 22 hours	<a href="#">Create Snapshot</a>
aw-server-0	(not found)	192.168.103.3 10.135.248.24	aw_low_tier_premium	aw-keypair	Active	fl-1 nova	None	Running	3 days, 22 hours	<a href="#">Disassociate Floating IP</a>
cp-sw-install-0	(not found)	192.168.101.11	m1.2xlarge	cp-keypair	Active	fl-1 nova	None	Running	2 weeks	<a href="#">Edit Instance</a>

Acknowledge the confirmation popup that displays.

- Select **Project > Orchestration > Stacks**.
- Select the AW Server specific stacks, and click on **Delete Stacks**.

#### NOTE

Do **NOT** remove the **aw\_port** stack. This will result in a reload of the entire EHL platform to reinstall the AW Server.

The screenshot shows the Horizon OAM Titanium Cloud interface under the Project > Orchestration > Stacks section. A table lists several stacks, including 'aw-server-0-volume-os' and 'aw-keypair' which are highlighted with a red box. The 'Actions' column for these stacks contains a 'Delete Stacks' button highlighted by a red box.

Stack Name	Created	Updated	Status	Actions
aw-server-0-volume-os	1 week, 1 day	1 week, 1 day	Create Complete	<a href="#">Check Stack</a>
aw-keypair	1 week, 1 day	1 week, 1 day	Create Complete	<a href="#">Check Stack</a>
aw-server-aw.low_tier_premium-0	1 week, 1 day	1 week, 1 day	Create Complete	<a href="#">Check Stack</a>

Acknowledge the confirmation popup that displays.

#### NOTE

If a stack deletion fails, redo the operation for this stack.

- Logout from Horizon OAM Titanium Cloud and login using **admin** credential.
- Select **Project > Orchestration > Stacks**.
- Select the AW Server specific stacks, and click on **Delete Stacks**.

The screenshot shows the Horizon OAM Titanium Cloud interface under the Project > Orchestration > Stacks section, logged in as the 'admin' user. A table lists several stacks, including 'aws-3.2-4.8' and 'aw\_low\_tier\_premium' which are highlighted with a red box. The 'Actions' column for these stacks contains a 'Delete Stacks' button highlighted by a red box.

Stack Name	Created	Updated	Status	Actions
aws-3.2-4.8	40 minutes	40 minutes	Create Complete	<a href="#">Check Stack</a>
aw_low_tier_premium	40 minutes	40 minutes	Create Complete	<a href="#">Check Stack</a>

Acknowledge the confirmation popup that displays.

### 2.29.3.5.2 Deploying the AW Server on a Virtual Machine

1. Insert the USB media with the preinstalled OS and AW Server into the Edison HealthLink.
2. Identify the USB media by typing the following command in the console/terminal of the Edison HealthLink:

```
sudo fdisk -l <Enter>
```

**NOTE**

The first time you use **sudo** command you may have to enter the **wrsroot** password.

The last USB media inserted will be **displayed as the last item** within the **Device Boot** section, in the output of the command.

```
Disk /dev/sdaa: 64.2 GB, 64160400896 bytes, 125313283 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xe637597e

      Device Boot      Start        End      Blocks   Id  System
/dev/sdaa1               128    125313250   62656561+   7  HPFS/NTFS/exFAT
controller-0:~$
```

Or, if the **Device Boot** section is empty, the USB media will be **displayed as the last Disk**.

```
Disk /dev/sdc: 32.2 GB, 32212254720 bytes, 62914560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x00000000

      Device Boot      Start        End      Blocks   Id  System
controller-0:/opt/backups$
```

Record the USB media name (here `/dev/sdc`), as it will be used in below commands.

3. Navigate to the `/opt/backups` directory:

```
cd /opt/backups <Enter>
```

4. Clean up the `ees/awserver` directory:

```
sudo rm -rf ees/awserver/* <Enter>
```

5. For versions EHL 1.5.2 and older, mount the USB media in read-only using the following command:

```
sudo mkdir -p mnt/awserver_package <Enter>
```

```
sudo mkdir -p mnt/usb_img <Enter>
```

```
sudo mount /dev/sdc mnt/usb_img <Enter>
```

**NOTE**

Here we assume that the USB partition is `/dev/sdc`. If it is not the case, replace `/dev/sdc` by the right USB partition as identified in [Step 2](#).

```
sudo mount -ro loop mnt/usb_img/aws-3.2-4.9-0.qcow2.iso \
mnt/awserver_package <Enter>
```

**NOTE**

The *qcow2.iso* file name used here, is the one from the Physical Software Kit. So, it is different if using a Digital Software Kit.

6. Create the Virtual Machine, deploy the AW Server and automatically configure the AW Server using the following command:

For versions EHL 1.5.2 and older:

```
edison vm -install /opt/backups/mnt/awserver_package <Enter>
```

From version EHL 1.5.3:

```
edison vm install <Enter>
```

Wait for the message "VM Installation successfully completed....." to display (roughly 5mn).

```
aw-server-0-volume-os Stack CREATE started
aw-server-0-volume-os Stack CREATE completed successfully
aw-server-aw.low_tier_premium-0 Stack CREATE started
aw-server-aw.low_tier_premium-0 Stack CREATE completed successfully
VM Installation successfully completed.....
controller-0:~$ [1012436.982885] kvm [5122]: vcpu0 unhandled rdmsr: 0x345
```

Press **<Enter>** to return to prompt.

7. For versions EHL 1.5.2 and older, unmount the USB partition:

```
sudo umount mnt/awserver_package <Enter>
```

```
sudo umount mnt/usb_img <Enter>
```

```
cd <Enter>
```

8. Remove the USB media from the Edison HealthLink:

Ignore the error message when removing the USB media.

Press **<Enter>** to return to prompt.

This completes the Virtual Machine creation with the AW Server deployment and the AW Server configuration.

### 2.29.3.5.3 Displaying the AW Server Console

The below steps described the process to display the AW Server Console from the Edison HealthLink.

1. In the Horizon OAM Titanium Cloud, select **Project > Compute > Instances**.

2. Click on **aw-server-0** in **Instance Name**.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
aw-server-0	(not found)	192.168.103.3	sw-lxc-tier-premium	hw-keypair	Active	a1	nova	None	Running	1 week, 1 day	<a href="#">Create Snapshot</a>
cp-grafana-0	65-centos7	192.168.101.18	a1.small	cd-keypair	Active	a1	nova	None	Running	3 weeks	<a href="#">Create Snapshot</a>

3. In the **Console** tab, click on **Click here to show only console**.

If console is not responding to keyboard input, click the grey status bar below. [Click here to show only console](#). To exit the fullscreen mode, click the browser's back button.

Connected (unencrypted) to: QEMU (instance-e-00000037)

The AW Server Console appears:

4. If the AW Server Console does not appear and the error message **503 Service Unavailable** appears:

- In the console/terminal of the Edison HealthLink, type:

```
cd tic_support <Enter>
sudo ./vnc_service_tool.sh <Enter>
```

The following message appears:

```
System is operational and enabled.
1) Enable_VNC_Console
2) Disable_VNC_Console
3) Quit
Please enter your number choice:
```

- Type:

```
1 <Enter>
```

The following message appears:

```
Removing security rule.
+-----+
| Property      | Value
+-----+
| uuid          | db26b919-4fe4-4544-9d0e-41e8745aa63f |
| firewall_sig  | 67ad602b11caf988a8d1cae14340ce01 |
| updated_at    | 2020-08-26 18:09:07.053625+00:00 |
+-----+
checking for multiple rules...
security rules cleared...
VNC will remain enabled only for 3 hours.
```

#### 2.29.3.5.4 Configuring the HA Proxy for AW Server

In order to be able to access the AW Server through the Edison HealthLink, the HA Proxy shall be configured to forward the ports needed by the AW Server.

Refer to the Edison HealthLink Site Installation Manual, section Application Software Installation, subsection For AW Server.

1. To configure the HA Proxy for AW Server, in the console/terminal of the Edison HealthLink, type the following commands:

```
cd /home/wrsroot/kindler/site_utils <Enter>
sudo ./haproxy_update.py awserver <Enter>
```

##### NOTE

In some Edison HealthLink version the `site_utils` folder may not exist and the command may have another extension. In this case type the following commands instead:

```
cd /home/wrsroot/kindler/shell_scripts <Enter>
sudo sh haproxy_update.sh awserver <Enter>
```

#### 2.29.3.5.5 Updating static routing file on AW Server

##### NOTE

This section is not applicable for the MR Smart Subscription on Edison HealthLink.

1. In the AW Server console, login as `root`.

##### NOTE

To display the AW Server Console, refer to [2.29.3.5.3 Displaying the AW Server Console on page 344](#).

2. Create the file `route-static-eth0` with the following text, as follow:

```
echo "172.16.0.0/24 via 192.168.103.254 dev eth0" >> /etc/sysconfig/
network-scripts/route-static-eth0 <Enter>
```

3. Restart the network service by typing the following command:

```
service network restart <Enter>
```

4. Confirm that the `172.16.0.0` has been added to the destination by typing the following command:

```
route <Enter>
```

```
[root@aws-08 network-scripts]# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
192.168.103.0   *              255.255.255.0  U     0      0        0 eth0
172.16.0.0      host-192-168-10 255.255.255.0  UG    0      0        0 eth0
link-local       *              255.255.0.0   U     1002   0        0 eth0
default         host-192-168-10 0.0.0.0     UG    0      0        0 eth0
[root@aws-08 network-scripts]#
```

5. Confirm that ping connectivity is successful by typing the following command:

```
ping 172.16.0.1 <Enter>
```

```
[root@aws-08 network-scripts]# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=63 time=1.31 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=63 time=0.172 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=63 time=0.177 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=63 time=0.194 ms
^C
--- 172.16.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3798ms
rtt min/avg/max/mdev = 0.172/0.465/1.318/0.492 ms
[root@aws-08 network-scripts]# _
```

6. To make the changes effective, type the following command:

```
/etc/sysconfig/network-scripts/ifup-routes static -eth0 <Enter>
```

7. Return to login mode by typing the following command:

```
exit <Enter>
```

### 2.29.3.5.6 Allocating floating IP address for AW Server

Allocate floating public IP address for the AW Server.

- Get the two Server IP addresses of the Edison HealthLink:
  - Login to Horizon OAM Titanium Cloud using **edison-usr** credential:
  - Select **Project > Network > Floating IPs**.

IP Address	Mapped Fixed IP Address	Pool	Status	Actions
172.16.0.120	-	external-net1	Active	<button>Disassociate</button>
10.135.248.25	-	external-net0	Active	<button>Disassociate</button>

- c. Record the following two IP Addresses:

- Edison proxy floating IP (external-net0): \_\_\_\_\_
- Edison private proxy floating IP (external-net1): \_\_\_\_\_

Refer to the Edison HealthLink Platform Service Guide, section Verify Edison IP Address.

2. Allocate Floating IP Address (Public) for AW Server:

- Move to **Project > Compute > Instances**.
- For **aw-server-0** instance, select **Associate Floating IP** in the pull-down menu.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
aw-server-0 (not found)	um-net0	192.168.103.3	aw.low_tier_premium	aw-keypair	Active	nova	None	Running	1 hour, 9 minutes	<a href="#">Create Snapshot</a>
cp-sw-install-0 (not found)	cp-net0	192.168.101.11	m1.2xlarge	cp-keypair	Active	nova	None	Running	1 week, 4 days	<a href="#">Edit Instance</a>

- Select the previously recorded allocated IP address that have been disassociated in Step 3 from section [2.29.3.5.1 Deleting the AW Server instance from the Edison HealthLink on page 341](#).
- Check that the new allocated Floating IP is added on the **aw-server-0**:

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status
aw-server-0 (not found)	um-net0	192.168.103.3 10.135.248.24	aw.low_tier_premium	aw-keypair	Active

- Move to **Project > Network > Floating IPs**.

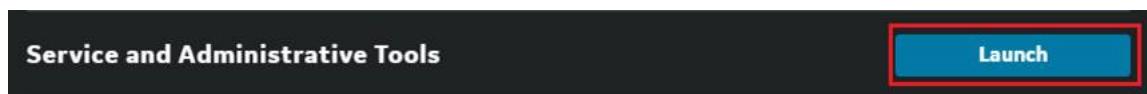
Confirm that the new allocated Floating IP address for AW Server is added at the **aw-server-0**:

The screenshot shows the WIND Titanium Cloud interface. The left sidebar has 'Project' selected under 'Compute'. The main area is titled 'Floating IPs' and displays a table with the following data:

	IP Address	Mapped Fixed IP Address	Pool	Status
<input type="checkbox"/>	172.16.0.120	-	external-net1	Active
<input type="checkbox"/>	10.135.248.25	-	external-net0	Active
<input type="checkbox"/>	10.135.248.24	aw-server-0 192.168.103.3	external-net0	Active

### 2.29.3.5.7 Launching Service Tools

1. Start the Services Tools from the FE laptop or the CT Console as done previously.
2. Click on the **Launch** button next to Service and Administrative Tools.



3. Log into the Service Tools as **service**.

### 2.29.3.5.8 Reviewing the network settings

1. From the Service Tools, select **Maintenance > Network**.
2. In the **IP address**, **Default gateway** and **Hostname** tabs, check the network information.

The three screenshots show the following network configurations:

- Configure system IP address:** Network interfaces: eth0, IP address: 192.168.103.3, Network prefix: 24. A 'Check IP' button is present.
- Configure default gateway:** IP address: 192.168.103.1. A 'Check IP' button is present.
- Configure system host name:** Hostname: aws, Domain name: (empty). A 'Check IP' button is present.

3. Update the network information if needed.

### 2.29.3.6 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.

The Service Pack is delivered in a Digital Software Kit. The Service Pack is compatible with electronic file delivery (eDelivery). The USB is prepared using the AW eDelivery Install Manager (AWeDIM) tool.

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

**NOTE**

For the systems connected via RSvP, if a new version of an AW Server Service Pack is available, it has been loaded onto the AW Server (from the software delivery portal).

**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.

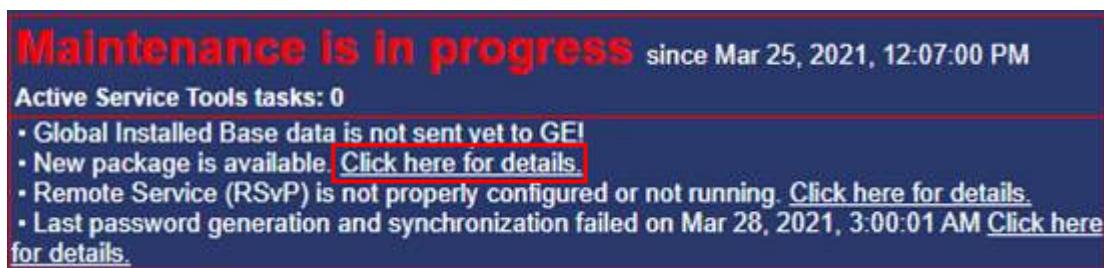
**NOTE**

It is **not** possible to uninstall a Service Pack.

### 2.29.3.6.1 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 [2.29.3.6.2 Installing the OS and AW Server Platform software Service Pack on page 352](#).

Otherwise, the AW Server Service Pack has been copied to USB media through the eDelivery mechanism.

**NOTE**

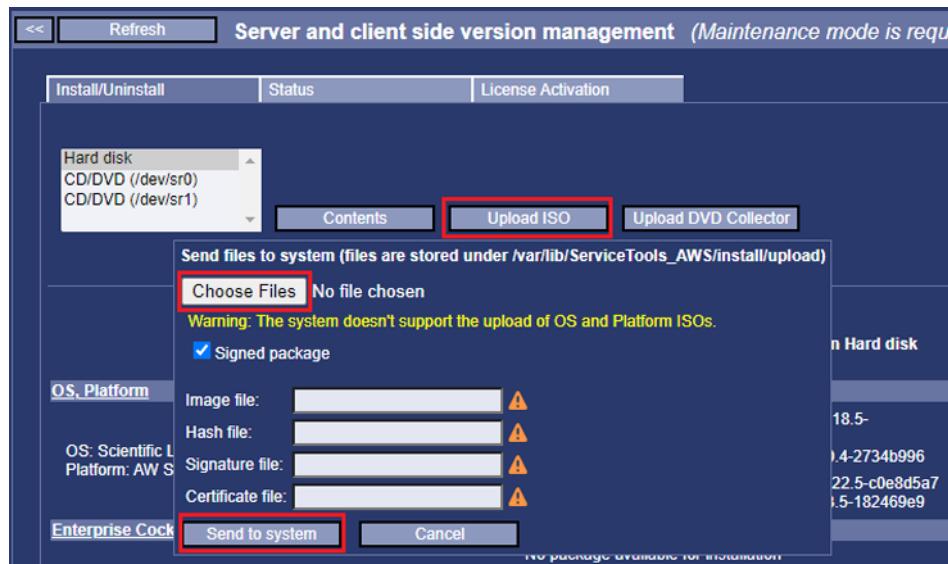
When loading from electronic files, always refer to *AW eDelivery Service Guide 5761599-8EN* for detailed instructions.

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**.
5. If the Service Pack ISO file is **signed**, follow the below substeps. Otherwise, jump to next step.

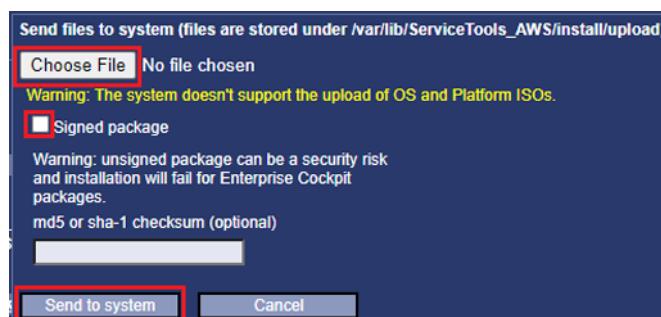
**NOTE**

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.

- 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).



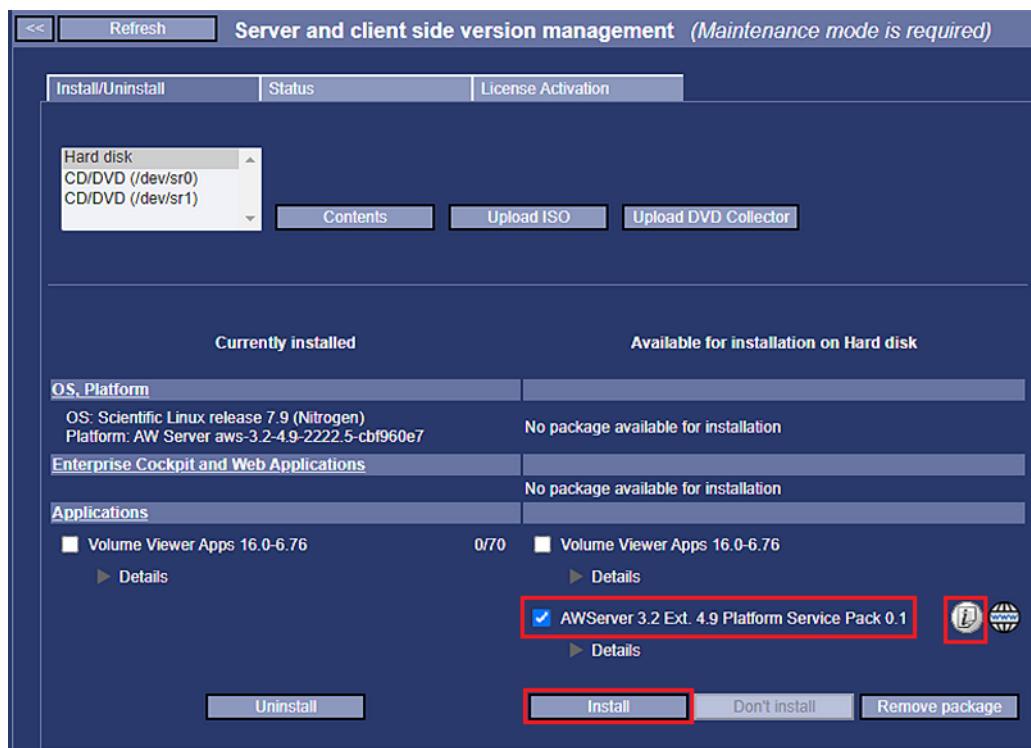
- The **Image file** (Service Pack ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
- If the Service Pack ISO file is **not signed**, follow the below substeps.
    - In the pop-up window, uncheck the **Signed package** check box.
    - 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.

## 2.29.3.6.2 Installing the OS and AW Server Platform software Service Pack

- Select the AW Server Service Pack to install and click on **Install**.



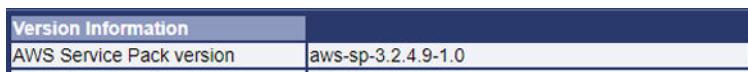
### NOTE

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.
- On the Healthpage, in **System Configuration** table, the **Modality OS Version** is updated.

Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9
Modality OS Version	AWS3.2_OS_7.2_SP_1.0 [20230109]
UDI	(01)00840682102384(10)AWS03D02E4D9SP1D0

- Reboot the AW Server.  
From the Service Tools, select **Tools > Reboot**, then select **Reboot AW Server**.  
Wait for the AW Server to reboot, then login again into the Service Tools.  
On the Healthpage, the **AWS Service Pack Version** displays in **Version Information**.

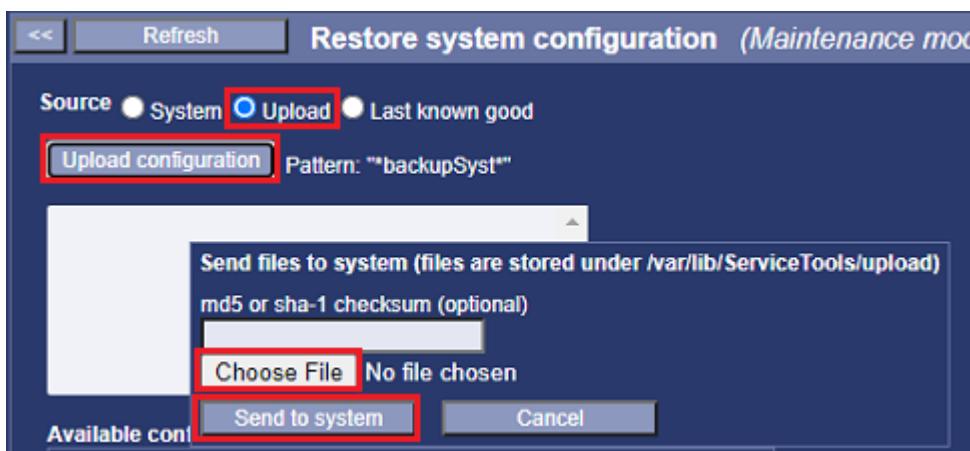
**NOTE**

If any issue occurs during the Service Pack installation or if the system does not work as expected after the Service Pack installation:

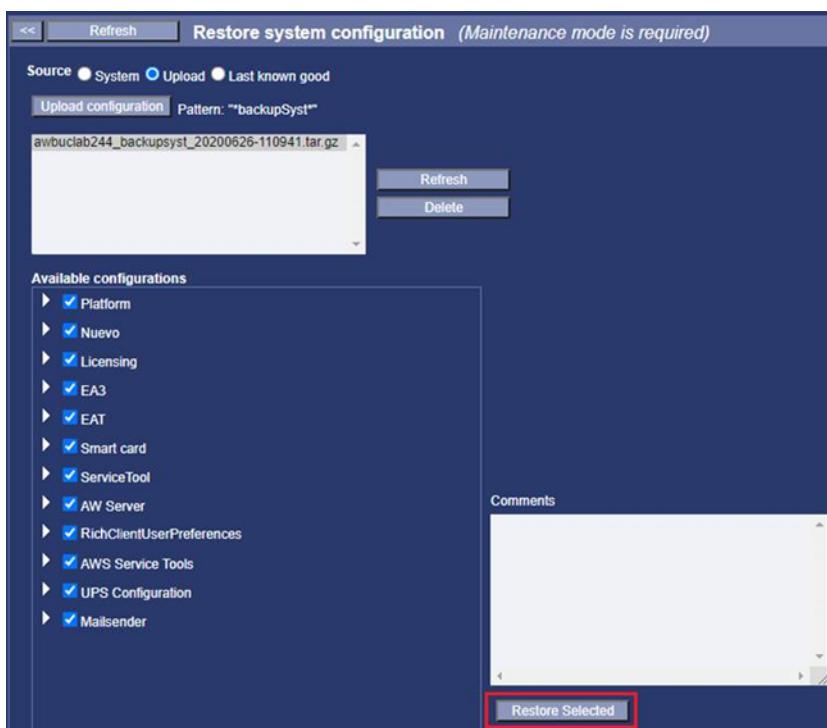
- Report the issue and contact an Online Service Engineer to collect the logfiles for further investigation.
- Use the backup created prior to install the Service Pack and reload the current AW Server (as for an upgrade – Load From Cold).

### 2.29.3.7 Restoring the saved configuration

1. From the Service Tools, select **Maintenance > Restore > System configuration**.
2. Upload the configuration file previously saved on your laptop or an USB media:
  - a. Select **Upload**.
  - b. Click on **Upload configuration**.  
A pop-up window appears.
  - c. Click on **Choose File**.
  - d. Choose the configuration file to upload and click on **Send to system**.  
When the upload is complete, a pop-up window appears.
  - e. Click on **OK**.



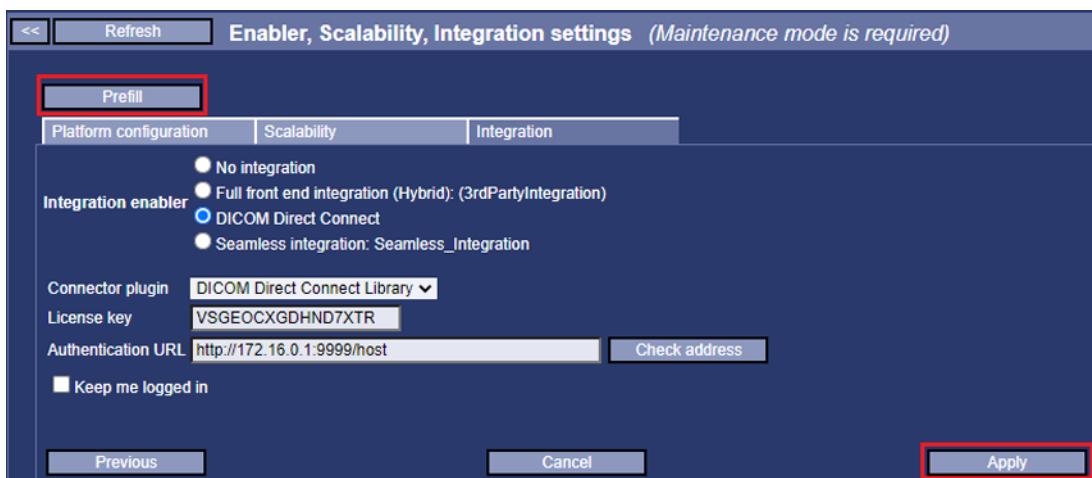
- Select the configuration previously uploaded, then click on **Restore Selected**.



### 2.29.3.8 Restoring the integration

The Platform configuration has been restored. However, it needs to be applied to be effective:

- From the Service Tools, select **Initial configuration > Platform Configuration**.
- Check that the **Platform license Key** displays.
- Click on **Next** twice to display the **Integration** tab.



- Click on the **Prefill** button to populate the integration parameters.

**NOTE**

If the integration parameters do not populate, enter them manually.

- Click on **Apply** to apply the platform configuration.

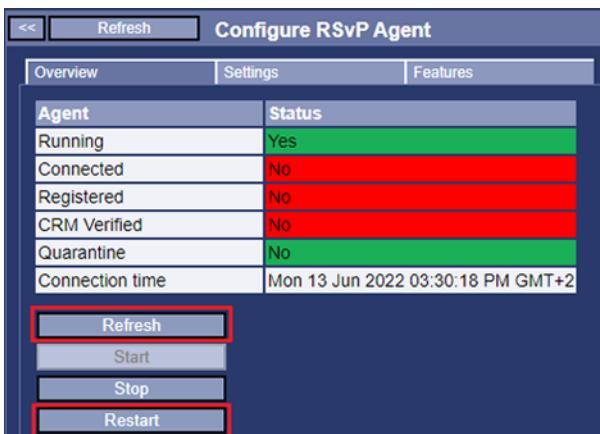
Acknowledge the confirmation popups that display.

The AW Server reboot will be done later.

### 2.29.3.9 Restarting the RSvP Agent

The Remote Connectivity has been restored (GEHC only). However, the RSvP Agent needs to be restarted.

- From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice)**.



- Click on the **Restart** button to restart the RSvP Agent.
- Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green.

### 2.29.4 Applications Installation/Upgrade

This section describes the steps to install/upgrade the applications on the AW Server.

The Applications are delivered either:

- In a Physical Software Kit.
- In a Digital Software Kit.

The Applications are compatible with electronic file delivery (eDelivery). The USB is prepared using the AW eDelivery Install Manager (AWeDIM) tool.

#### NOTE

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

#### NOTE

For the systems connected via RSvP, if a new version of the Applications are available, they have been loaded onto the AW Server (from the software delivery portal).

#### NOTE

This section requires to use the AW Server Service Tools. If they have been closed, refer to [2.29.2.9.1 Launching Service Tools on page 327](#) and [2.29.2.9.2 Navigating in Service Tools on page 330](#) to launch them.

#### NOTE

The AW Server requires to be placed in Maintenance Mode before any application installation/upgrade. If not already done in previous section, refer to [2.29.3.3 Entering the Maintenance Mode on page 338](#), to place the AW server in Maintenance Mode.

#### NOTE

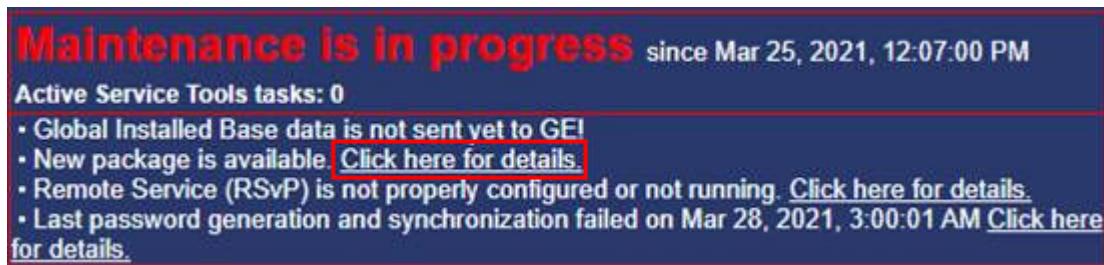
Repeat the below sections for any applications purchased by the customer (e.g.: Volume Viewer, SmartScore, ...).

## 2.29.4.1 Loading the applications

This section describes how to load the applications (for a new installation) or to load new version of the applications.

For the systems connected via RSvP, if new applications versions are available, they have 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 install the applications in [2.29.4.2 Installing the applications on page 357](#).

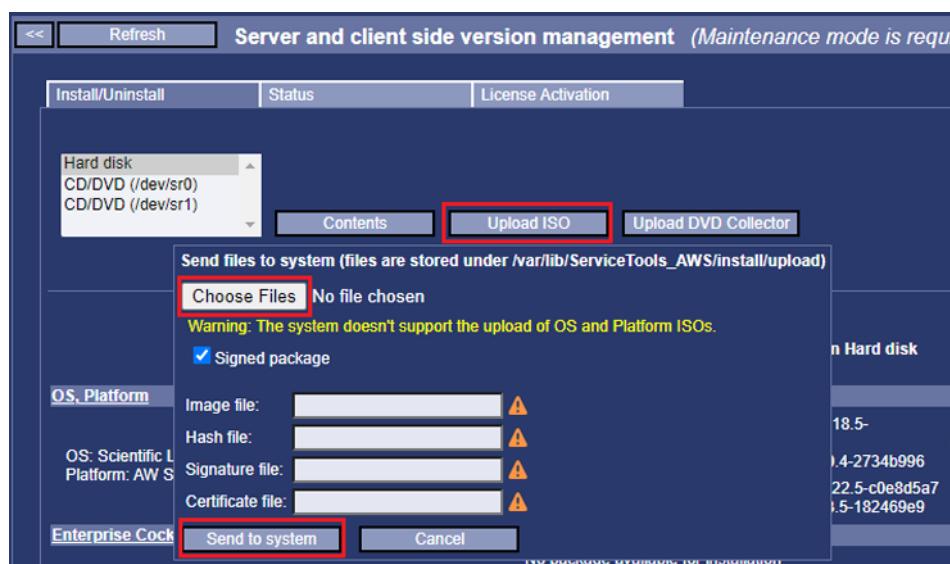
Otherwise, the Applications are available on USB media.

1. Insert the USB media into 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**.
5. If the application ISO file is signed, follow the below substeps. Otherwise, jump to next step.

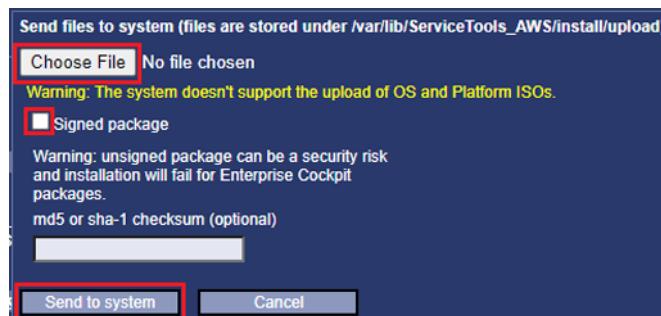
### NOTE

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.

- a. In the pop-up window click on **Choose File** and select the 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).



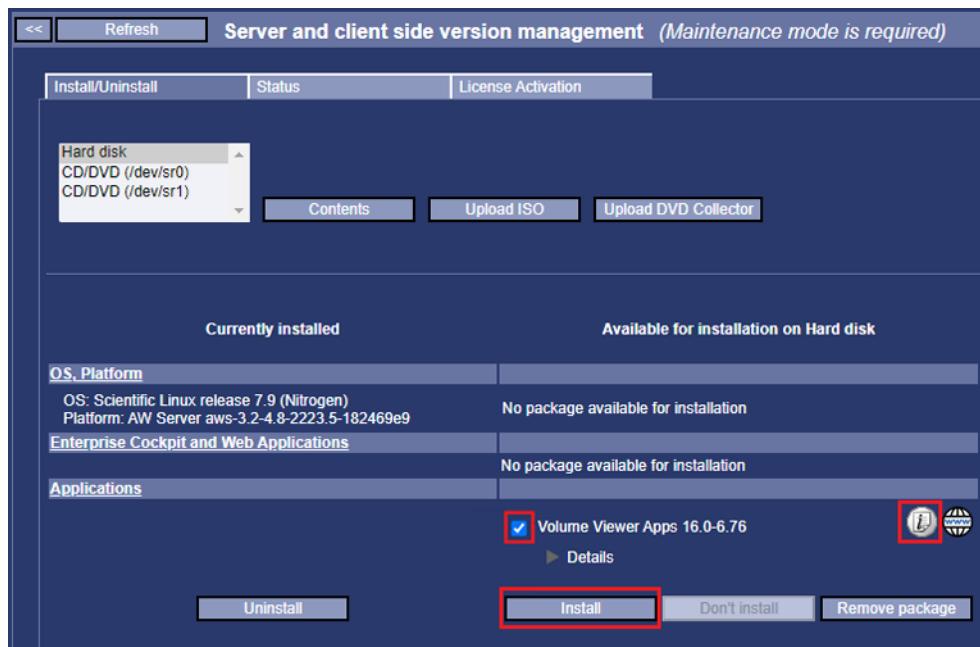
- b. The **Image file** (component ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
- 6. If the application ISO file is not signed, follow the below substeps.
  - a. In the pop-up window, uncheck the **Signed package** check box.
  - b. Click on **Choose File** and select the ISO file stored on the media.



- c. 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.
  - 7. To upload the ISO file, click on **Send to system**.
- When the upload is completed, acknowledge the popup that displays.
8. Verify that the application appears in the *Available for installation on Hard disk* part of the page.
  9. Remove the media from the FE laptop.

## 2.29.4.2 Installing the applications

1. Select the application to install and click on **Install**.



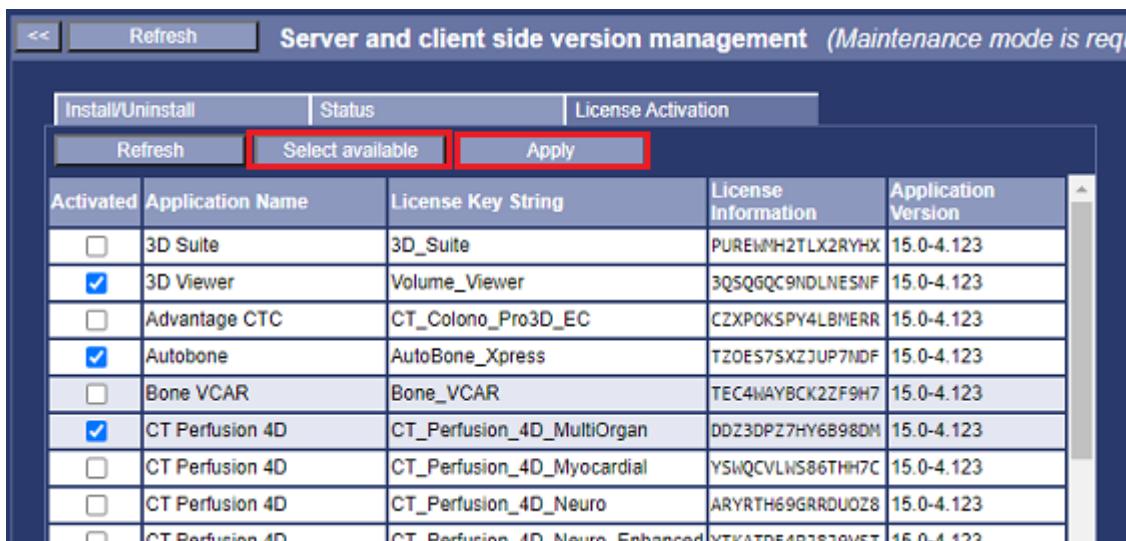
### NOTE

For the systems connected via RSvP, if new applications versions are available, they have 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.

2. 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.
3. Select the **Install/Uninstall** tab.
4. Check that the application appears in the *Currently installed* part of the page.

### 2.29.4.3 Activating the applications

1. Select the **License Activation** tab.
2. Click on **Select available** to automatically check the boxes of all licensed applications available on the Floating License Server.
3. Click on **Apply** to activate the application licenses.



Install/Uninstall		Status	License Activation	
Refresh		Select available	Apply	
Activated	Application Name	License Key String	License Information	Application Version
<input type="checkbox"/>	3D Suite	3D_Suite	PUREMH2TLX2RYHX	15.0-4.123
<input checked="" type="checkbox"/>	3D Viewer	Volume_Viewer	3Q5QQQC9NDLINESNF	15.0-4.123
<input type="checkbox"/>	Advantage CTC	CT_Colono_Pro3D_EC	CZXPOKSPY4LBMR	15.0-4.123
<input checked="" type="checkbox"/>	Autobone	AutoBone_Xpress	TZ0ES7SXZJUP7MDF	15.0-4.123
<input type="checkbox"/>	Bone VCAR	Bone_VCAR	TEC4WAYBCK2ZF9H7	15.0-4.123
<input checked="" type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_MultiOrgan	DDZ3DPZ7HY6B98DM	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Myocardial	YSWQCVLWS86THH7C	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Neuro	ARYRTH69GRRDUOZ8	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Neuro_Enhanced	VTVATDAD1810VST	15.0-4.123

#### NOTE

If no change occurs (no new application have been installed), the **Apply** button remains greyed out and there is no need to reactivate the applications.

4. Remove the USB media from the FE Laptop.

### 2.29.5 AW Server final Settings

This section describes the final settings prior to handover the AW Server to customer.

#### NOTE

This section requires to use the AW Server Service Tools. If they have been closed, refer to [2.29.2.9.1 Launching Service Tools on page 327](#) or [2.29.3.1 Launching Service Tools on page 335](#) to launch them.

#### NOTE

If only application(s) have been installed/upgraded, perform only sections [2.29.5.2 Registering the system configuration on page 366](#), [2.29.3.4 Backing up the configuration on page 341](#) and [2.29.5.4 Exiting maintenance mode on page 368](#).

#### NOTE

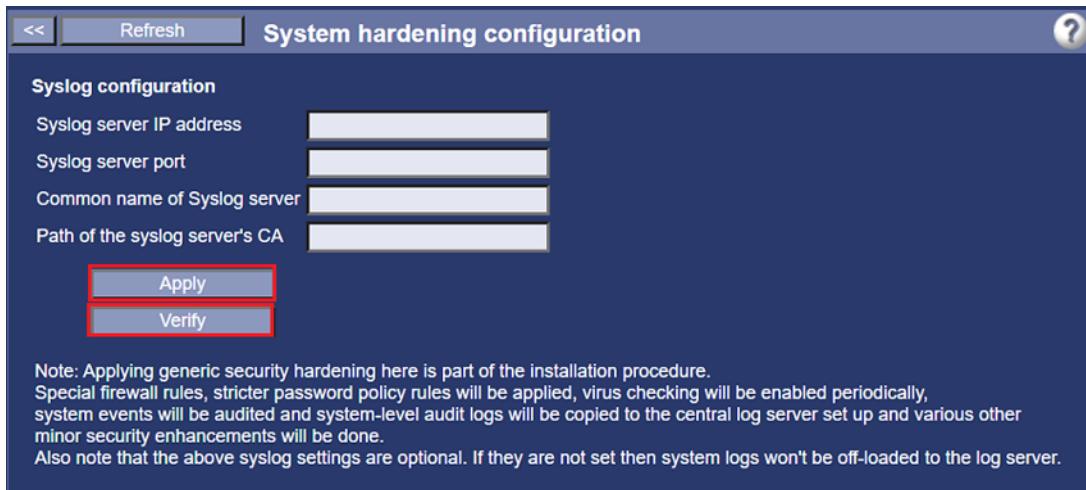
To check the AW Server configuration or to manually configure the AW Server (for instance, in case the automatic configuration with the Installation Wizard (Cloud-init mechanism) did not work during AW Server deployment) or for any additional settings on the AW Server, please refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#) and [2.18 Job Card IST010 - Administrative Configuration on page 184](#).

## 2.29.5.1 Security settings

### 2.29.5.1.1 System Hardening

Improve the security of the system by enforcing the local user account password rules:

- From the Service Tools, select **Initial configuration > Hardening**.



- Leave the **Syslog configuration** fields empty and click on **Apply** button and then on **Verify** button.

### 2.29.5.1.2 Changing the Passwords

The account 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 passwords.

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

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 requires that the server's system 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. **No system shall be handed over to the customer with the default root password under any circumstances.**

**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.**

#### NOTICE

When changing the passwords DO NOT MISS to notify the OLC representatives. Failing to do so would no longer allow access to your system from the OLC support teams.

### 2.29.5.1.2.1 Passwords Change Procedure

## 2.29.5.1.2.1.1 Identifying New Password(s)

The customer may request specific passwords. If this is the case, get the passwords from the customer and move on to [2.29.5.1.2.1.2 Changing Linux passwords on page 361](#). Make sure that the passwords chosen by the customer comply with the rules listed below.

### NOTE

For the systems connected via RSvP, the passwords for **root** and **filetransfer** Linux users/accounts, are generated and synchronized with the RSvP server (GE Backoffice), as described in [2.29.5.1.2.1.2 Changing Linux passwords on page 361](#).

If a new password is to be created, the FE should do so in the following ways:

- If required, use customer rules and guidelines for password creation.
- If the FE is free to choose the password, use the following guidelines:
  - Must be 8 to 15 characters min. and 63 characters max.
    - 8 characters min. for AW Server user passwords (default value that can be changed)
    - 15 characters min. for Linux passwords
  - Must contain 1 digit
  - Must contain 1 upper-case letter
  - Must contain 1 lower-case letter
  - Must contain 1 non-alphanumeric character
  - Must not be a palindrome
  - Must not be blank or left as the default
  - Must not be made up solely of dictionary words or easily guess
  - Must not contain 3 consecutive identical characters
  - Must not contain a blank space
  - Must not include your logon name
  - Should not be the same value at different sites

Good password examples:	Bad password examples:
<b>!414585MR5test\$</b>	<b>414555AWS5</b>
<b>4\$42CTAWServer32</b>	<b>operator</b>
<b>big996622LS16ct*</b>	<b>123456789a</b>

The following characters (which the system may assign a special meaning) should be avoided:

**@ ; # ; <Tab> ; <Esc>** ; etc .... However, **#** can be used for the **root** password.

### NOTICE

Each account on a single system should have a unique password. For example, the **root** and **admin** accounts should have different password values from each other. Using the same password for multiple accounts on a system will remove role-based access and decrease the level of security on a system.

For productivity, the same password value for a single account can be used on multiple systems at a site or customer. For example, the **root** user/account could have the same non-default password value on 3 different systems in a hospital. However, make sure not to use the same value over multiple sites or across a region, because that would essentially duplicate the original default

value problem this service note attempts to resolve. For this reason, procedures are given below for alternative AW platform releases.

### 2.29.5.1.2.1.2 Changing Linux passwords

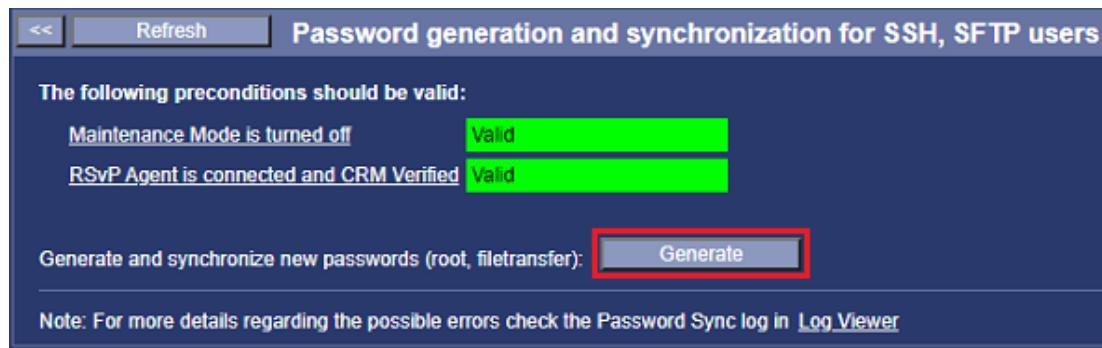
To change the passwords for **root** / **filetransfer** Linux users/accounts follow the below steps:

1. If the system is connected via RSvP, the passwords for **root** and **filetransfer** Linux users/accounts, can be generated and synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault:

#### NOTE

In case of a full AW Server installation the Linux passwords can be changed later as the Configuration must be registered prior to turn off the Maintenance Mode

- a. From the Service Tools, select **Administrative > Configuration > Users (OS)**.



- b. The Maintenance Mode must be turned off. If the status is **Invalid**, click on **Maintenance Mode is turned off** to open the *Server maintenance tasks* page. In this page, select **Finish maintenance**.
- c. The RSvP Agent must be connected and CRM Verified. If the status is **Invalid**, click on **RSvP Agent is connected and CRM Verified** to open the RSvP configuration page. Refer to [2.29.2.9.3 Setting up Remote Service on page 330](#).
- d. Click on the **Generate** button to generate the new passwords for **root** and **filetransfer** Linux users/accounts and synchronize them with the RSvP server (GE Backoffice).
- e. Remotely through FFA, display the *System Password Vault* panel.

The screenshot shows a "System Password Vault" interface. At the top, it says "Showing 3 configured accounts for System ID AWBUCLAB162". Below is a table with columns: #, App Name, Username, Password, Last Updated, Updated By, and Actions. The table rows are:

#	App Name	Username	Password	Last Updated	Updated By	Actions
1	ea3	service	*****	Feb-17-2021 12:02:58	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
2	sftp	filetransfer	*****	Feb-18-2021 12:10:59	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
3	ssh	root	Uz\$Un3f+ONaznezA SiM.UwwiMKi	Feb-18-2021 12:11:10	AGENT	<a href="#">Hide</a> <a href="#">Copy</a> <a href="#">Change Password</a>

- f. Select the **Show** link to view the new password.

**NOTE**

New passwords are generated and synchronized on a weekly basis, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified.

2. If the system is not connected via RSvP, the Linux passwords for **root** can be changed using a command line window:
  - a. Open a command window:
    - via the **Service Tools > Tools > Terminal**,
    - or via the **SSH** connectivity tool or the **Terminal** tool in FFA.
  - b. Login as **root**, using the current **root** password.
  - c. To change the current password, type:  
**passwd <Enter>**
  - d. Type the new password and press **<Enter>**.
  - e. To confirm the new password, type it again and press **<Enter>**.
  - f. Logout and login again to apply the change.
3. It is STRONGLY RECOMMENDED to test the new passwords before turnover to customer, in order to make sure that there was no typo or mix-up with the local keyboard when the password was changed.
  - a. Open another command-line window.
  - b. Login with each Linux users/accounts and enter the new passwords.

The operating system is configured to lock accounts for a minimum of 15 minutes after five unsuccessful logon attempts within a 15-minute timeframe. The operating system is configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds. Do not use the **authconfig** tool in the operating system for authentication configuration, it may overwrite the system hardening settings.

**NOTE**

This fail lock mechanism does not apply to the **root** Linux user account.

### 2.29.5.1.2.1.3 Changing AW Server Users Password(s)

**NOTE**

A secure password policy is set for default EA3 local users and the passwords must be changed (if not already changed) during installation: **admin**, **limited**, **standard** and **service** password.

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

After the password is identified, the FE should make the password changes on the device.

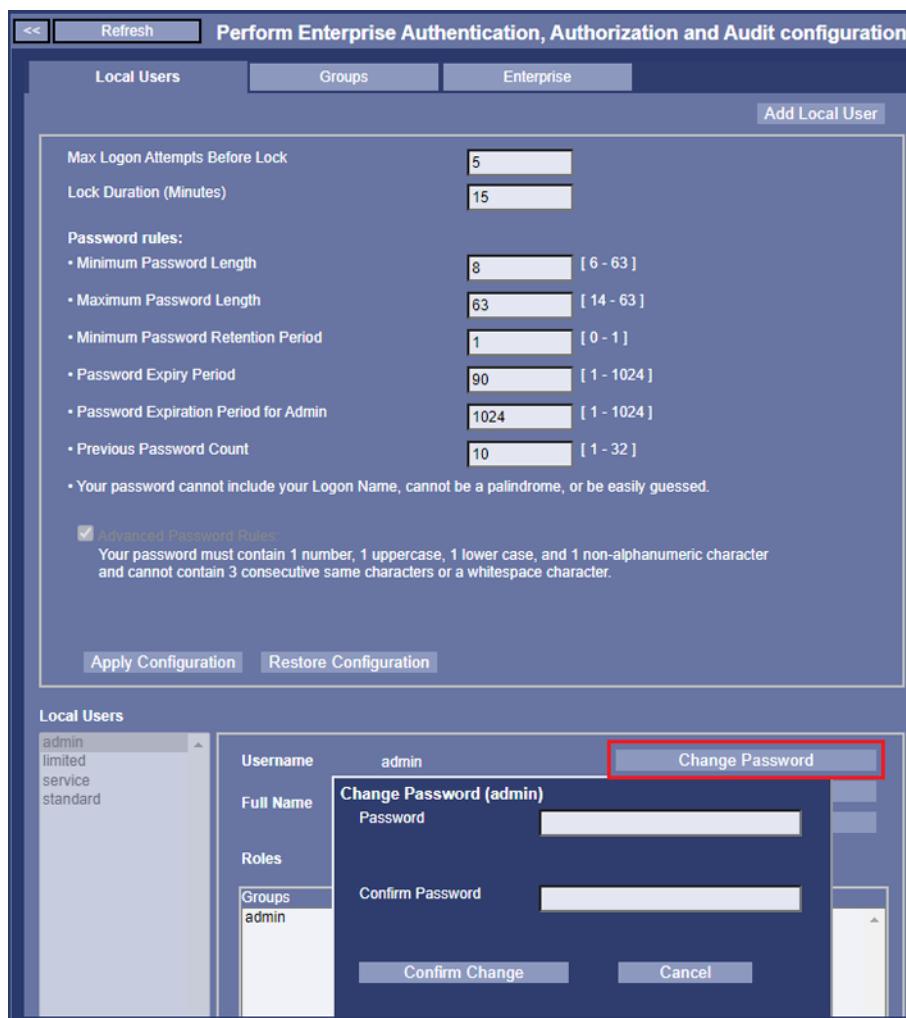
There are **Four** default AW Server users accounts, for which the passwords require change:

- **service** (Permanent account)
- **admin** (Removable account)
- **standard** (Removable account)
- **limited** (Removable account)

The AW Server is configured to lock accounts for a minimum of 15 minutes after five unsuccessful logon attempts.

## 2.29.5.1.2.1.3.1 Changing the passwords from the EA3 local users page

- From the Service Tools, select **Administrative > Configuration > Users (EA3)**.



- In the **Local Users** area, select a user account and click on the **Change Password** button.
- In the **Change Password** window enter the new password and confirm it.

### NOTE

The default password rules can also be changed in this page.

- To confirm the new password, click on **Confirm Change**.
- To change another user's password, repeat the procedure (from Step 2 to Step 4).
- To force the password change at the next login (AW Server Client login), check the **Change Password on Next Login** check box.



### NOTE

After an upgrade, as the passwords are restored to the default values and/or the password policy may have changed, the password shall be changed. So, check the **Change Password on Next Login** check box.

7. Click on **Apply Configuration** button.

### 2.29.5.1.2.1.3.2 Synchronizing the service password with RSvP

If the system is connected via RSvP, the **service** password is synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified:

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 <a href="#">Change Password</a>
2	sftp	filetransfer	*****	Jun-14-2021 19:07:31	AGENT	Show  Copy <a href="#">Change Password</a>
3	ssh	root	*****	Jun-14-2021 19:07:34	AGENT	Show  Copy <a href="#">Change Password</a>

2. Select the **Show** link to view the new password.

### 2.29.5.1.2.2 Updating Password(s) in Connectivity Database

Update the password in the Connectivity Database and notify the OLC representatives, as described in the table below.

Region	Connectivity Center Information
AMERICAS (US, Canada)	USCAN Connectivity Support toll-free number: 877-842-1132 (8am – 6pm CST, Mon-Fri)
LatAm	Preferably reach the connectivity team via <a href="https://sc.ge.com/*LATAMcheckout">https://sc.ge.com/*LATAMcheckout</a> 
EU and EMEA	Use the Support Central EMEA Password Change workflow <a href="https://sc.ge.com/*emeapwc">https://sc.ge.com/*emeapwc</a> 
Japan	Call the Connectivity Support number: 0120 596 919

ASEAN	Contact OLE or connectivity champion for re-checkout the system.
ANZ	Call the Connectivity Support numbers Australia 1800 659 465 or New Zealand 0800 659 465 OR open a case at <a href="http://sc.ge.com/*ANZConnectivity-Support">http://sc.ge.com/*ANZConnectivity-Support</a>
Korea	Call the Connectivity Support (OLC support) number : 1544 6119
China	Call the Connectivity Support number : 400 812 8188 OR contact OLE for system checkout/re-checkout
India	Call the Connectivity Support number : 1800 102 7750 (India Call Center) ext 4

### 2.29.5.1.2.3 Communicating New Password(s)

1. Follow your customer's guidelines for password communication and storage. Inform the customer of the new passwords with the exception of those used for remote service only.
2. If the customer approves, write down the new passwords and store them in a secure location on site.  
The [2.29.5.1.2.4 Password Form on page 365](#) includes a sample form to place in a logbook or tape inside a cabinet.
3. In the situation where a customer wants to know more about what GE does with passwords, escalate to the service security team at:  
[http://supportcentral.ge.com/products/sup\\_products.asp?prod\\_id=295163](http://supportcentral.ge.com/products/sup_products.asp?prod_id=295163)

### 2.29.5.1.2.4 Password Form

 GE Healthcare

Password Change Record for  
System ID \_\_\_\_\_  
By \_\_\_\_\_  
Date \_\_\_\_\_

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Copyright Pending

The passwords configuration is complete.

## 2.29.5.2 Registering the system configuration

- From the Service Tools, select **Maintenance > Register Configuration**.

The screenshot shows the 'Register Configuration' page with the following sections:

- Status** (Left Column):
  - licenseld:** 068abc98
  - Registration Key status:** Registration Key : BSADDRNRJYFMNAGB, Registration Status : Invalid
  - Connectivity Status :** Configuration Registration(AWCCT) Server not reachable
- Install Registration Key** (Top Right):
  - Registration Key :
  - If you have a valid Registration Key, enter it in the field above to complete registration
- Auto Register** (Middle Right):
  - Perform Auto Registration** button (highlighted with a red box)
  - If the system is connected to GE (InSite), click this button to export configuration to AWCCT. If configuration is valid, a Registration Key is returned and automatically installed on the workstation.
- Export Configuration (Manual Registration)** (Bottom Right):
  - Export Configuration** button (highlighted with a red box)
  - Instructions :**
    - If the system is not connected to GE, and valid Registration Key not available:
      - Click button above to export the configuration file to Hard disk
      - Upload this file to <https://awcct.gehealthcare.com> to get a Registration Key. If you cannot connect from the system, try from a PC with internet access.
      - Install the Registration Key on the system to enable software/applications

- Automatic Registration:

If the AW Server is connected via RSvP and that the System ID (CRM Number) is verified, you can use the Automatic Registration process.

- Click on the **Perform Auto Registration** button, to automatically send the Site configuration file to the AWCCT Web site.

If the configuration is compliant, messages will say so in the **Connectivity Status** and **Registration Status** areas on the left of the page and you will automatically receive in return within a few seconds the Registration key, while at the bottom left of the page, the message Request in progress appears, followed by Operation success.

- The **Registration status** field in the HealthPage should display as Standard in green.

Bypass the next steps. They are dedicated to manual registration when remote connection via RSvP is not available.

- Manual Registration:

If the AW Server is NOT connected via RSvP, perform a manual registration.

- Click on **Export Configuration** to export the configuration file on your laptop.

- b. In an Internet Navigator connect to <https://awcct.gehealthcare.com> and upload the configuration file:

Submit Advantage Workstation Configuration File(AW/AW Server/AW Pioneer)

Select configuration file to Upload : *	<input type="button" value="Choose File"/> 068abc98_...nfiguration.txt
Any Comments/Suggestions :	
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- i. Click on **Choose File**, then select the configuration file previously exported.
  - ii. Click on **Submit** to generate the registration key.
- | File Name   | File Upload Status | Registration Key                             | System ID   | License ID | View Details               |
|---|--------------------|--|-------------|------------|----------------------------|
| 068abc98_AWBUCLAB240_100005286_AWS_20201230160121.txt | Success            | <input type="text" value="FNKLOZJIBXDJIHJ"/> | AWBUCLAB240 | 068abc98   | <a href="#">Click here</a> |
- c. Type in the registration key into the **Registration Key** field and click on **Install Registration Key**.

Install Registration Key

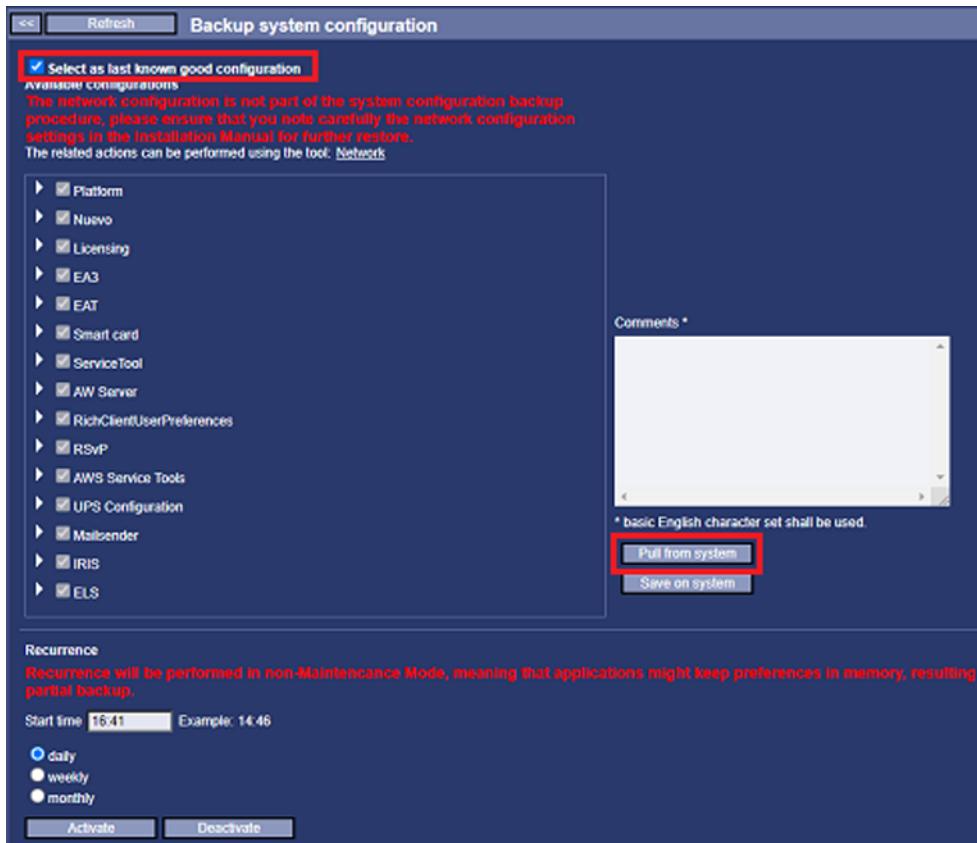
Registration Key :

If you have a valid Registration Key, enter it in the field above to complete registration

At the bottom left of the page, the message Request in progress appears, followed by Operation success.

### 2.29.5.3 Backing up the configuration

- From the Service Tools, select **Maintenance > Backup > System configuration**.

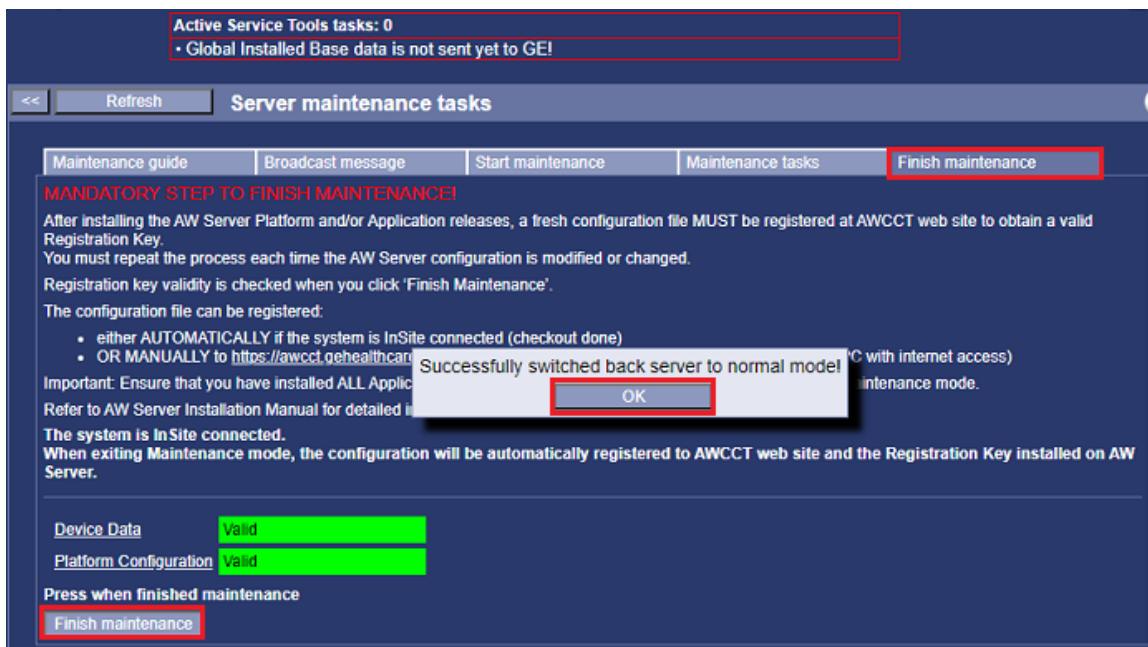


- Check the **Select as last known good configuration** radio button.
- Keep everything selected and click on **Pull from system** to save the configuration on the local system.
- Copy the saved configuration on an USB media and keep it in a safe place.

### 2.29.5.4 Exiting maintenance mode

- From the Service Tools, select **Maintenance > Maintenance > Finish maintenance**.
- Click on **Finish maintenance**.

3. In the pop-up window, click **OK**.



## 2.29.5.5 Accessing AW Server through HA proxy or external IP addresses

To access the AW Server through HA Proxy or external IP addresses, a script should be executed.

1. In the AW Server Console, login as **root**.

To display the AW Server Console, refer to [2.29.2.4 Displaying the AW Server Console on page 321](#).

2. Execute the script below for the DICOM hosts configured in this procedure:

```
cd /opt/keycloak/bin <Enter>
```

```
./set_multiple_host_configs.py <Edison Proxy Floating IP>
<host2>...<Enter>
```

For Instance:

```
./set_multiple_host_configs.py 10.135.248.25 <Enter>
```

OR

```
./set_multiple_host_configs.py <new allocated Floating IP for AW Server>
<host2>...<Enter>
```

For Instance:

```
./set_multiple_host_configs.py 10.135.248.24 <Enter>
```

### NOTE

A **<host>** can be an IP address, an IP address with a specified port or a fully qualified domain name.

## 2.29.6 AW Server feature connection – CT Console

This section describes the AW Server Client installation/update and configuration in the CT Console, and check the AW Server Client connectivity.

**NOTE**

The AW Server Client is already installed with the CT option key [Smart Subscription – Connection].

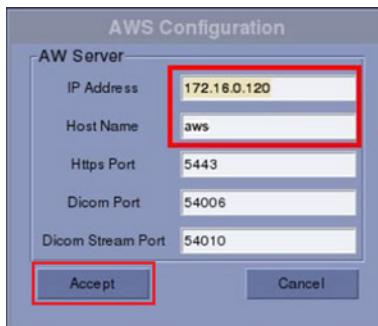
1. Install the [Smart Subscription – AW Server] CT option. Refer to the Smart Subscription Service Manual.

**NOTE**

The [Smart Subscription – Connection] CT option key must be installed prior to installing the [Smart Subscription – AW Server] CT option.

The AW Server Configuration window displays.

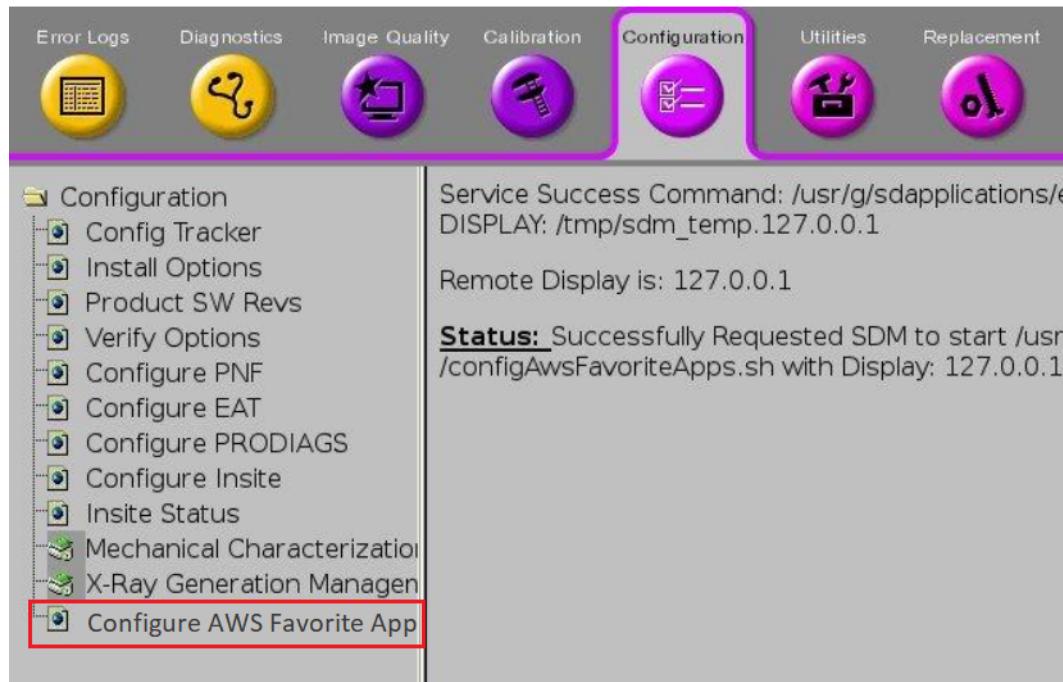
2. Enter the Edison Private Proxy Floating IP in the **IP Address** field and the AW Server host name, that was **set up during the AW Server installation**, in the **Host Name** field. Then click on **Accept**.



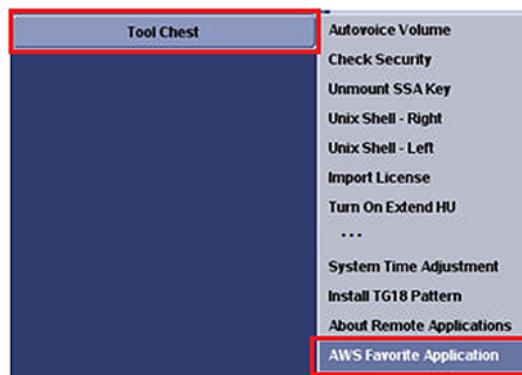
3. Reboot the CT Console.
4. Display the **AWS Favorite Application** window.

Depending on the CT Console type:

- a. Either, switch to the **Service** desktop and start the Service Desktop interface using the CSD tool, then select **Configuration > Configure AWS Favorite Application**.



- b. Or, in the **Tool Chest** pull-down Menu, select **AWS Favorite Application**.



- c. In the **AWS Favorite Application** window select your applications then click on **Accept**.



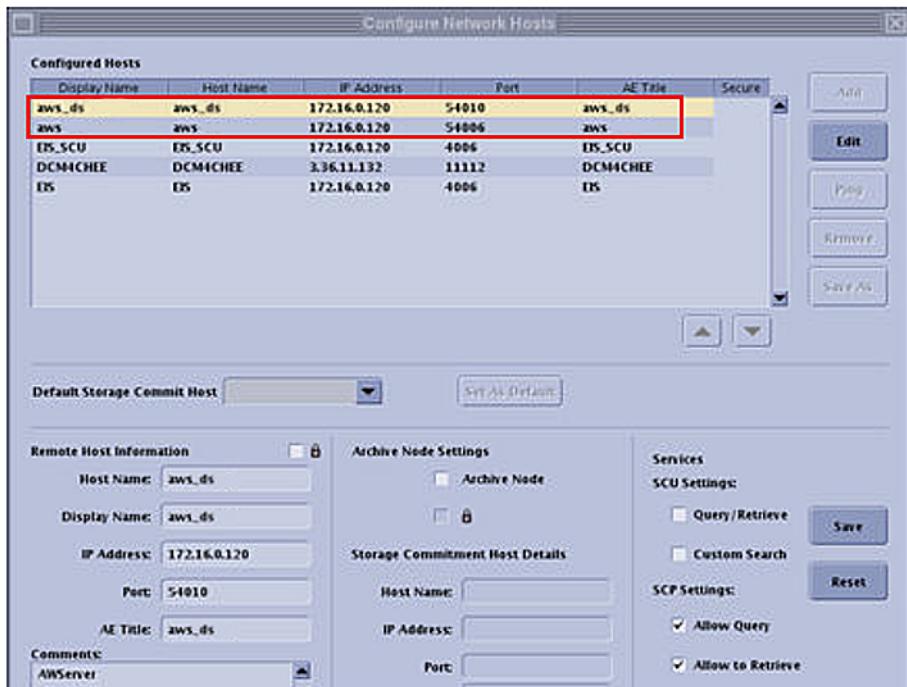
#### NOTE

Refer to the project manager to select the applications available for your site.

5. Check the network configuration:

- a. Switch to the **ImageWorks** desktop.

- b. Select **Tools > Network Configuration** and check that two Remote Hosts are present for the AW Server.



## 6. Check AW Server Client connectivity:

- Switch to the **ImageWorks** desktop.
- In the Browser, select a scan instance.
- Select an application prefixed by **AWS** (for instance **AWS Reformat**). The application starts.

### NOTE

Acknowledge the popup window related to certificate if any.



## 2.29.7 Installing the AW Server Client in MR Console

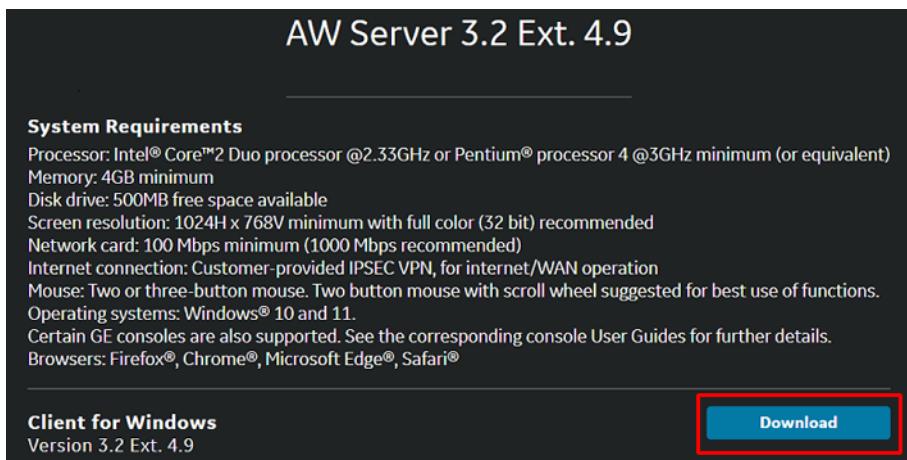
All steps are performed and completed by the GE FE.

### NOTE

For the MR Console, the AW Server Clients are installed on the customer desktops/laptops.

1. Launch the Service Tools.

Refer to [2.29.2.9.1 Launching Service Tools on page 327](#).



2. Review the system requirements for the client displayed on the AW server main page.
3. Click on the **Download** button next to Client for Windows to download the installed file for the AW Server Client.
4. When the installer file is downloaded completely and saved on the desktop, double-click the corresponding icon to run it.

The Windows setup wizard interface appears.

5. Follow the steps to install the AW Server Client.

This completes the AW Server Client installation/update.

## 2.30 NanoCloud AW Server Installation in CT Console

The AW Server can be installed in a Virtual Machine running on the CT Console. It is called the NanoCloud AW Server (also called NanoCloud AWS or Nano AWS).

### Important

The NanoCloud AW Server shall be installed using English language. If the CT Language setting is not in English, please change it to English prior to installing the NanoCloud AW Server. Once the installation is complete, CT languages setting can be changed as needed.

In this environment, the CT Console hosts the AW Server Virtual Machine. It allows users to do advanced processing with AW Applications remotely from the CT Console.

The OS and AW Server software are packaged in a pre-installed image available on USB device and used to install and configure the AW Server.

The AW Server is configured in the DICOM Direct Connect mode and retrieves the patients/images data from the CT Console database.

The AW Server Client is integrated within the CT Console Client.

### NOTE

Always refer to the relevant service documentation for details:

- The CT service documentation.
- This Service Manual.

Prerequisite:

- Installation of the CT Console software has been completed.

- USB Media containing the combined OS and the AW Server qcow2 image template is necessary.
- USB Media with Volume Viewer Application is necessary.

#### **NOTE**

In the below sections, when requested to use a USB media (for configuration or licenses file generation), always use a GE validated read/writeable USB media.

#### **Important**

After the start/restart of the CT Console, the AW Server is usually available 5 to 10 minutes later. This is only an estimated time, and the actual delay will vary depending on the hardware host and CT Console configuration.

The below sections described:

- The installation and/or upgrade of a NanoCloud AW Server on the CT Console.
- The installation and/or upgrade of the applications on top of the NanoCloud AW Server.
- The installation of patches to fix critical vulnerabilities and bugs (Service Pack) on top of the NanoCloud AW Server.

In the below sections you are guided to the right sections/sub-sections depending on the type of installation/upgrade.

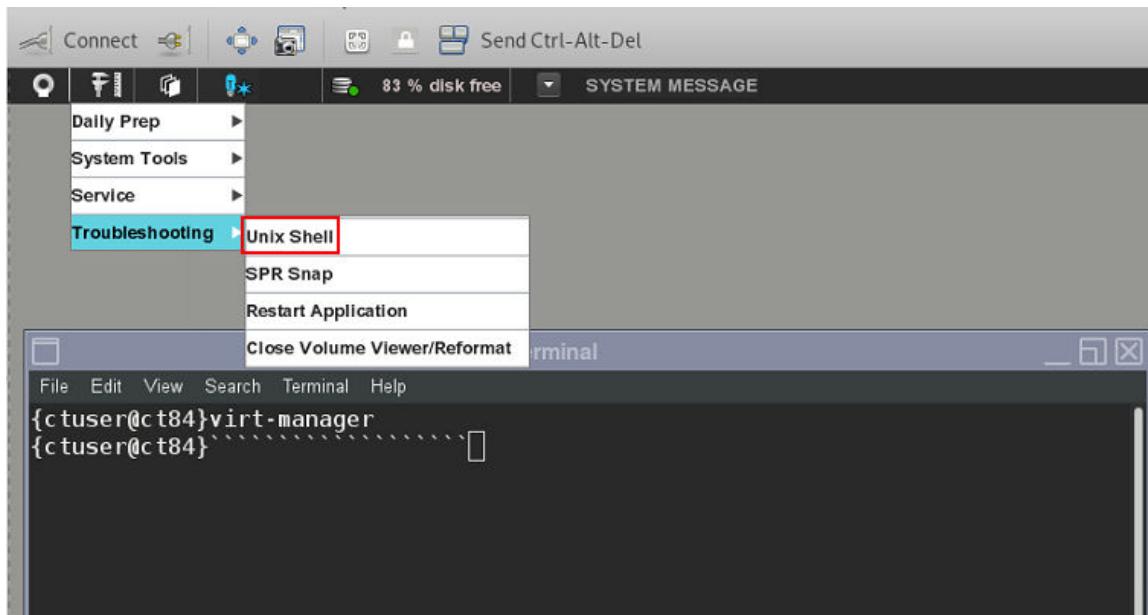
All sections are performed and completed by the GE FE.

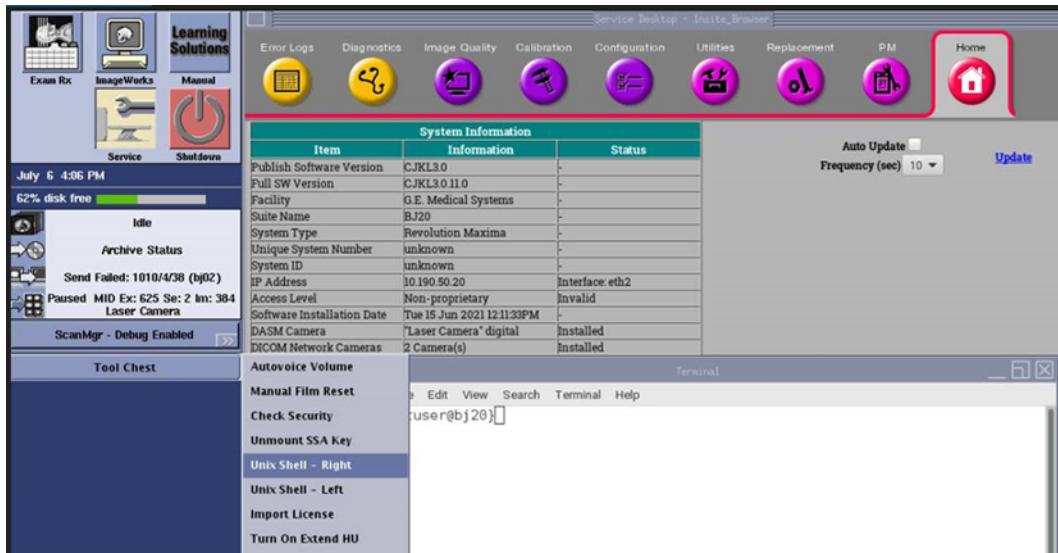
## **2.30.1 Installation/Upgrade Preparation**

This section describes the steps to prepare the NanoCloud AW Server (AW Server and/or Applications) installation or upgrade.

### **2.30.1.1 Opening a console/terminal on the CT Console**

1. Open a Unix Shell (console/terminal) on the CT Console. The below captures show how to proceed depending on the type of CT Console:





2. Login to the console/terminal using the **ctuser** credential.

Refer to the CT Console documentation.

#### **NOTE**

In the following sections, you are asked to login as **root** or **ctuser**. To know who you are, type in the command **whoami**. If the result is **ctuser** and you are asked to be **root**, type in the command **su root** and enter the password. If the result is **root** and you are asked to be **ctuser**, type in the command **exit**.

#### **Important**

DO NOT CLOSE THE TERMINAL BEFORE AW SERVER DEPLOYMENT AND CONFIGURATION COMPLETION

## 2.30.1.2 AW Server files Preparation

#### **Important**

Follow this section only for a **Load From Cold of the CT Software** or an **upgrade** of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to copy the AW Server image file and the associated checksum into the laptop.

The AW Server software is delivered using two methods:

- [Physical Software Kit on page 23](#) (USB media obtained from manufacturing or through parts):

Part Number	Content	Purpose
5818084-10 (or higher)	aws-3.2-4.9-0.qcow2.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.
	aws-3.2-4.9-0.qcow2.iso.sha256	This file contains the reference checksum of the above file, to verify its integrity.

- [Digital Software Kit on page 25](#) (files downloaded via eDelivery):

File name (in eDelivery Software Portal)	Purpose
5865570-5_AW_Server-3.2_Ext.4.9_and_OS_QCOW2_Template_for_VM.iso	This iso file is used for <b>Initial Installation &amp; Upgrade/Update</b> on the CT/MR Console Environment.

<b>File name (in eDelivery Software Portal)</b>	<b>Purpose</b>
<i>packagemetadata.json</i>	This file contains the reference checksum of the above file, to verify its integrity.

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

1. On the laptop, create a folder and name it AWS\_EXT4.9.

2. In case of Physical Software Kit:

- a. Insert the AW Server USB media into an USB port of the laptop.
- b. Copy the following files into the AWS\_EXT4.9 folder:

*aws-3.2-4.9-0.qcow2.iso*

*aws-3.2-4.9-0.qcow2.iso.sha256*

- c. Remove the USB media from the laptop.

3. In case of Digital Software Kit (files downloaded via eDelivery):

- a. Download the following files from eDelivery into the AWS\_EXT4.9 folder:

*5865570-5\_AW\_Server\_3.2\_Ext.4.9\_and\_OS\_QCOW2\_Template\_for\_VM.iso*

*packagemetadata.json*

- b. Rename the *5865570-5\_AW\_Server\_3.2\_Ext.4.9\_and\_OS\_QCOW2\_Template\_for\_VM.iso* file to *aws-3.2-4.9-0.qcow2.iso*.

4. Calculate the qcown iso file checksum:

**`certutil -hashfile aws-3.2-4.9-0.qcow2.iso SHA256 <Enter>`**

5. Display the qcown iso file checksum:

- In case of Physical Software Kit:

Open the *aws-3.2-4.9-0.qcow2.iso.sha256* file using Notepad editor.

- In case of Digital Software Kit:

The checksum is present in the *packagemetadata.json* file. Open the file and search for qcown iso file name.

The checksum calculated in Step 4 and the checksum shown at this time must be the same. If it is not the case, copy the AW Server image file into the laptop again.

### 2.30.1.3 Installation Tool files Preparation

#### Important

Follow this section only for a **Load From Cold of the CT Software** or an **upgrade** of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to copy the Installation Tool files and directories into the laptop.

The Installation Tool is delivered in a [Digital Software Kit on page 25](#) (files downloaded via eDelivery):

<b>File name (in eDelivery Software Portal)</b>	<b>Purpose</b>
5940647-AW_Server_3.2_Ext.4.9_Install_Tool.zip	This compressed package is used for Initial <b>Installation &amp; Upgrade/Update</b> to prepare the AW Server configuration.

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

1. On the laptop, if not already done, create a folder and name it AWS\_EXT4.9.
2. Download the 5940647-AW\_Server\_3.2\_Ext.4.9\_Install\_Tool.zip file from eDelivery into the AWS\_EXT4.9 folder.

## 2.30.1.4 Applications files Preparation

**Important**

Follow this section only for the **installation or upgrade of Applications** on top of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to copy the Applications iso files and their associated checksum into the laptop.

The Applications are delivered using two methods:

- Physical Software Kit (USB media was obtained from manufacturing or through parts).
- Digital Software Kit (files downloaded via eDelivery).

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

**NOTE**

For the AW Server connected via RSvP, if a new version of the Applications are available, they have been loaded onto the AW Server (from the software delivery portal). In this case ignore the below steps to copy the files into the laptop.

1. On the laptop, if not already done, create a folder and name it AWS\_EXT4.9.
2. In case of Physical Software Kit:
  - a. Insert the Applications USB media into an USB port of the laptop.
  - b. Copy the Applications files into the AWS\_EXT4.9 folder:

For instance for a Volume Viewer application, copy the following files:

AWE-Voxtool-vxtl\_16.0-6.84.x86\_64.iso  
AWE-Voxtool-vxtl\_16.0-6.84.x86\_64.iso.sha256

- c. Remove the USB media from the laptop.
- d. Calculate the Application iso file checksum:

For instance, for a Volume Viewer application:

```
certutil -hashfile AWE-Voxtool-vxtl-16.0-6.84.x84_64.iso SHA256  
<Enter>
```

- e. Open the Application iso file checksum.

For instance, for a Volume Viewer application, using Notepad editor open:

**AWE-Voxtool-vxtl-16.0-6.84.x84\_64.iso.sha256**

The checksum calculated in [Step 2.d](#) and the checksum shown at this time must be the same. If it is not the case, copy the Application image file into the laptop again.

3. In case of Digital Software Kit (files downloaded via eDelivery):

- Download the Applications files from eDelivery into the AWS\_EXT4.9 folder.

For instance for a Volume Viewer application, download the following files:

5871339-4\_Volume\_Viewer\_Apps\_16.0\_Ext.\_6\_SW\_and\_Docs\_for\_AW\_Workstation\_and\_AW\_Server.zip  
packagemetadata.json

- Calculate the Application zip file checksum.

For instance, for a Volume Viewer application:

```
certutil -hashfile  
5871339-4_Volume_Viewer_Apps_16.0_Ext._6_SW_and_Docs_for_AW_Workstation_and_AW_Server.zip SHA256 <Enter>
```

- Display the Application zip file checksum.

The checksum is present in the packagemetadata.json file. Open the file and search for the application zip file name.

The checksum calculated in [Step 3.b](#) and the checksum shown at this time must be the same. If it is not the case, copy the Application zip file into the laptop again.

4. Repeat the above steps for any applications purchased by the customer (e.g.: Volume Viewer, SmartScore, ...)

## 2.30.1.5 Service Pack file Preparation

### Important

Check the available patches (Service Packs) in eDelivery and download the latest Service Pack of this AW Server version.

Follow this section **only** for the **installation of patches** (Service Pack) on top of the **NanoCloud AW Server**. Otherwise, **skip** this section.

A Service Pack is a patch that allows to fix critical vulnerabilities and bugs in the AW Server software and the underlying OS.

This section describes the steps to copy the Service Pack iso file and its associated checksum into the laptop.

The Service Pack is delivered in a Digital Software Kit (files downloaded via eDelivery).

### NOTE

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

### NOTE

For the systems connected via RSvP, if a new version of an AW Server Service Pack is available, it has been loaded onto the AW Server (from the software delivery portal). In this case ignore the below steps to copy the file into the laptop.

- On the laptop, if not already done, create a folder and name it AWS\_EXT4.9.
- Download the Service Pack files from eDelivery into the AWS\_EXT4.9 folder:

For instance for an AW Server patch, copy the following files:

5925560\_AW\_Server\_3.2\_Ext.4.9\_Service\_Pack\_1.0.zip  
packagemetadata.json

3. Calculate the Service Pack zip file checksum:

For instance:

```
certutil -hashfile AWServer_3.2_Ext.4.9_Platform_Service_Pack_0.1.zip
SHA256 <Enter>
```

4. Display the Service Pack zip file checksum.

The checksum is present in the `packagemetadata.json` file. Open the file and search for the Service Pack zip file name.

The checksum calculated in [Step 3](#) and the checksum shown at this time must be the same. If it is not the case, copy the Service Pack zip file into the laptop again.

5. Repeat the above steps for any other Service Pack.

## 2.30.1.6 Generating the eLicenses file

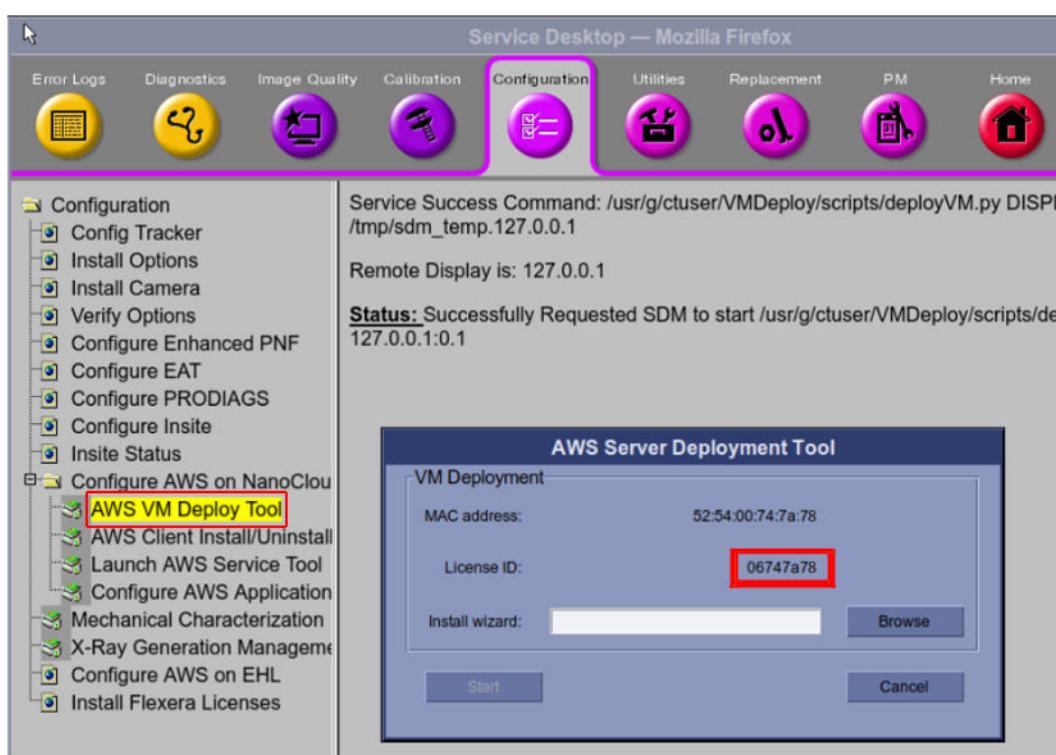
### Important

Follow this section only for a **Load From Cold of the CT Software**. Otherwise, **skip** this section.

This section describes the steps to generate the eLicenses file on the laptop.

1. Get the license ID:

From the CT Console, in the Service Desktop interface using the CSD tool, select **Configuration > Configuration AWS on NanoCloud > AWS VM Deploy Tool**.



2. Get the site System ID or GON (Global Order Number) listed on the site's paperwork from GE HealthCare.
3. Generate the eLicenses file on your laptop:

Refer to [A.3 Licensing on page 556](#) for the complete procedure.

The GE HealthCare eLicense website from <http://elicense.gehealthcare.com/elicense/> OR <http://elicense.gehealthcare.com/> - this URL is available via the Internet, and via the GE HealthCare VPN connectivity model.

**NOTE**

If you cannot connect to eLicense, contact the OLC and ask them to obtain the licensing information for you.

4. Copy the eLicenses file into the AWS\_EXT4.9 folder.

### 2.30.1.7 Copying the files prepared on the laptop into an USB media

This section describes how to copy the files prepared on the laptop into an USB media.

**NOTE**

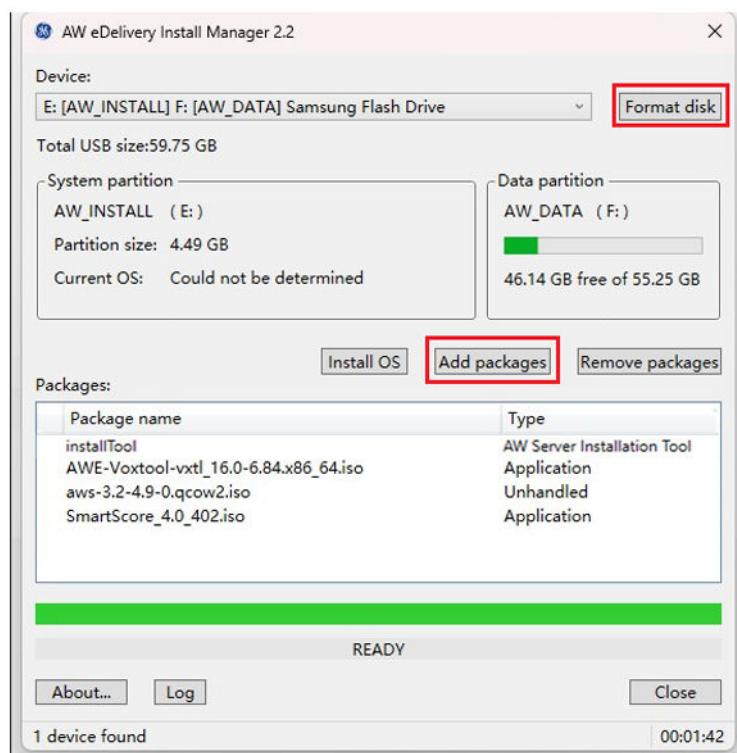
For the USB media, use at least a 32 GB USB media.

1. Copy the *iso* and/or *zip* files from the EXT4.9 folder into the USB media, using the AWeDIM tool.

**NOTE**

When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

- a. Download the AWeDIM tool from eDelivery and install it on the laptop.
- b. Insert the USB media into an USB port of the laptop.
- c. Start AW eDelivery Install Manager.



- d. Click on **Format** to format the USB media.
- e. Use **Add packages** to add *iso* and/or *zip* files previously copied in the EXT4.9 folder into the USB media.

**NOTE**

The zip files will be unzipped by the AWeDIM tool. The Installation Tool zip file may appear as *ffjext.zip*, however it is actually unzipped.

**NOTE**

When adding the *qcow2 iso* file a popup may display mentioning that the file is damaged. Ignore the message and acknowledge the popup.

f. Click on **Close**.

You can view the files copied into the USB media by opening the AW\_DATA partition of the USB media.

2. If applicable, copy the eLicenses file into the AW\_DATA partition of the USB media.

## 2.30.2 AW Server Installation

### Important

Follow this section only for a **Load From Cold of the CT Software**. Otherwise, **skip** this section.

This section describes the steps to install, deploy and configure the NanoCloud AW Server from the USB media.

### NOTE

After the first **installation** of the **NanoCloud AW Server**, continue with section [2.30.4 AW Server Service Pack Installation on page 415](#).

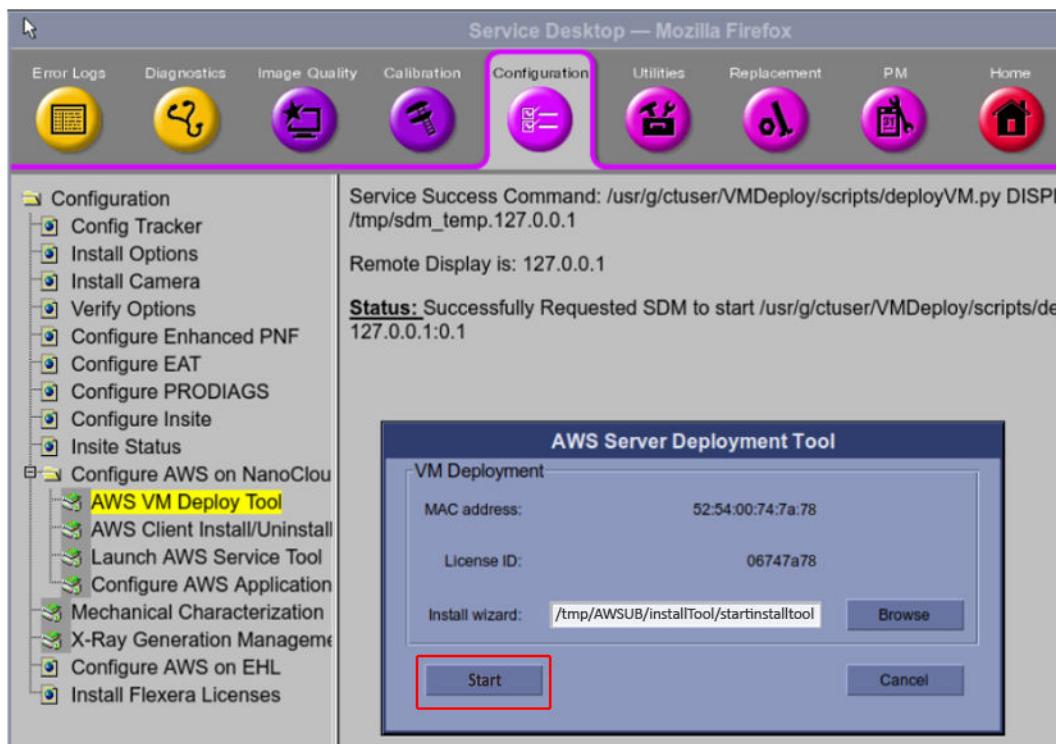
### 2.30.2.1 Preparing and deploying the AW Server with the AW Server Installation Tool

The AW Server Installation Tool allows to prepare and perform the basic AW Server configuration. It generates a configuration file that can be interpreted by the AW Server to perform the configuration automatically during its first start. The Installation Tool allows then to deploy the AW Server in a Virtual Machine of the CT Console.

#### 2.30.2.1.1 Launching the AW Server Installation Tool

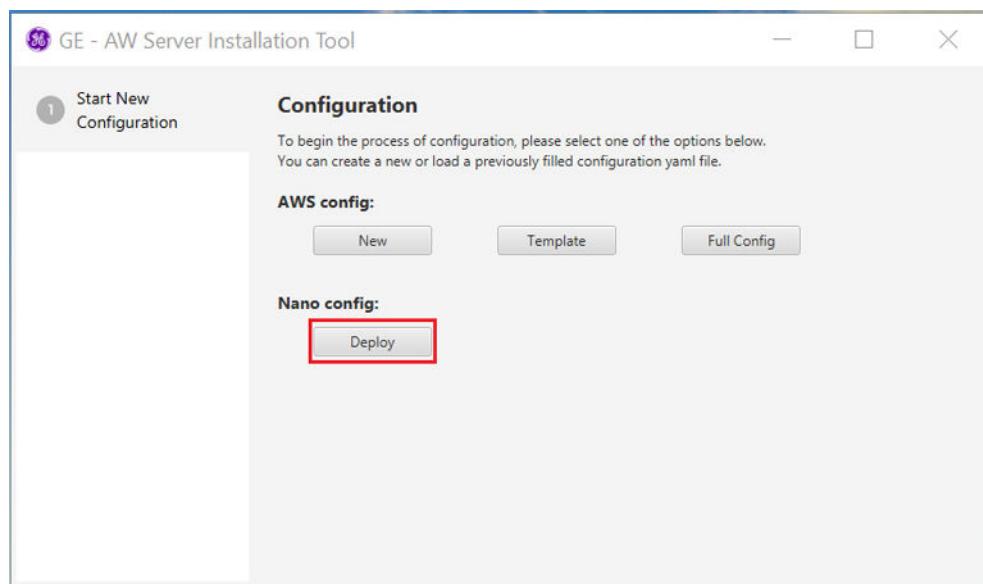
1. Insert the USB media into the CT Console.
2. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > AWS VM Deploy Tool**.

The **AWS Server Deployment Tool** window displays.



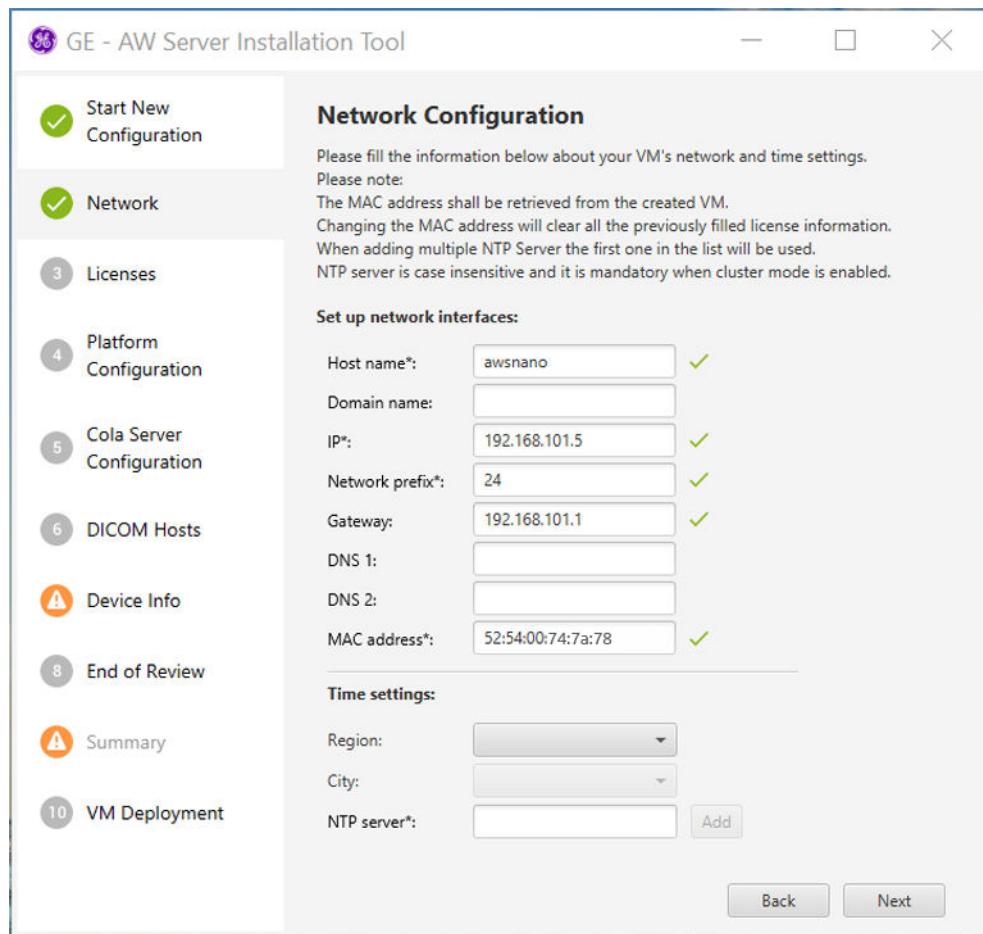
- Click on **Start** button.

The AW Server Installation Tool appears.



- In the **Start New Configuration** tab, click on **Deploy**.

The **AW Server Installation Tool** displays the different tabs used to configure the AW Server and move to the **Network** tab.



### 2.30.2.1.2 AW Server Installation Tool navigation and Field Filling Rules

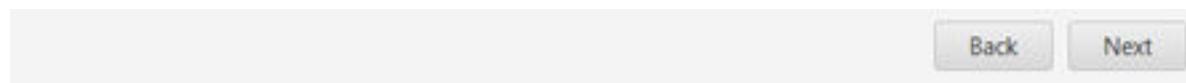
In the following steps all fields marked with an asterisk (\*) are mandatory and must be filled out. Other fields are optional.

If a field is wrongly filled, the symbol  appears next to the field and also on the corresponding tab and the *Summary* tab, as shown in the example below.

When all the mandatory fields are correctly filled, a green check appears near the fields and on the tab, as shown in the example below:

 Network	Set up network interfaces: Host name*: awsnano ✓ Domain name: <input type="text"/> IP*: 192.168.1015  Network prefix*: 24 ✓	 Network	Set up network interfaces: Host name*: awsnano ✓ Domain name: <input type="text"/> IP*: 192.168.101.5 ✓ Network prefix*: 24 ✓
Field wrongly filled (here the IP field)		Field correctly filled	

To navigate through the tabs click directly on the tab or on the **Next** and/or **Back** buttons at the bottom right of the Installation Tool.



#### NOTE

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#), to know the characters rules and limitations of the specific fields (Hostname, AE Title, IP Address, Port, System ID, Label/Name).

### 2.30.2.1.3 Configuring the network and time settings

- In the **Network** tab, most of the network information are prefilled. Check the **Host name**, the **IP** address, the **Network prefix**, the **Default Gateway** and the **MAC address**.

#### Network Configuration

Please fill the information below about your VM's network and time settings.

Please note:

The MAC address shall be retrieved from the created VM.

Changing the MAC address will clear all the previously filled license information.

When adding multiple NTP Server the first one in the list will be used.

NTP server is case insensitive and it is mandatory when cluster mode is enabled.

#### Set up network interfaces:

Host name*:	awsnano ✓
Domain name:	<input type="text"/>
IP*:	192.168.101.5 ✓
Network prefix*:	24 ✓
Gateway:	192.168.101.1 ✓
DNS 1:	<input type="text"/>
DNS 2:	<input type="text"/>
MAC address*:	52:54:00:74:7a:78 ✓

#### Time settings:

Region:	Europe
City:	Paris
NTP server*:	<input type="text"/> Add

- In the *Time settings* panel, select the **Region** and the **City**.

3. The **NTP server**'s IP address is not mandatory.
4. Click on **Next**.

#### 2.30.2.1.4 Configuring the licensing settings

1. Click on the **Browse** button and locate the eLicenses file in the /tmp/AWSUB directory.

The screenshot shows two main sections of the CT Console interface:

- Generate eLicenses:** A section where users are instructed to generate licenses from the e-license website using a provided License ID. It displays the MAC address of NIC 1 (52:54:00:74:7a:78) and a License ID (06747a78). A "Copy" button is available for the License ID. Below this, there's a link to "Go to eLicense Site".
- Add eLicences:** A section for uploading eLicenses. It includes a "License file:" input field containing the path /tmp/AWSUB/config-06747a78.txt, a "Browse" button (which is highlighted with a red box), and a "Remove All" button. Below this is a table titled "Uploaded Licenses" showing two entries:

License Name	License Key
AutoBone_Xpress	ZU3C7MOCNJ7N9XS3
Volume_Viewer	3SU9AYMOXVBKNPYX

2. Select the eLicenses files then click on **Open** to load the file.  
The licenses appear in the *Upload Licenses* list.
3. Click on **Next**.

#### 2.30.2.1.5 Configuring the platform settings

In the **Platform Configuration** tab, the Platform Integration Mode is filled based on the imported eLicense file.

1. Check the **Authentication URL** and the **Console host IP address**. They are based on the **Gateway** filled in [2.30.2.1.3 Configuring the network and time settings on page 383](#).

## Platform Configuration

The Platform Configuration is automatically filled based on the imported license file. Please review and select the appropriate configuration and fill out the remaining information if needed.

Note : Console Host IP address field is only for Nano licenses.

### Platform Integration Mode

Standalone

DICOM Direct Connect  
(PACSinteg plugin)

Platform enabler\*: SdC\_Nano\_12k

Platform license key\*: NTPJSUQKHR7ZMZYA

Integration license key\*: ZU3C7MOCNJ7N9XS3

Authentication URL:

Console host IP address\*:  ✓

Preprocessing license key (AutoLaunch): Not set

2. Click on **Next**.

### 2.30.2.1.6 Configuring the license server(s) settings

In the **Cola Server Configuration** tab, the License Server configuration is automatically filled based on the imported eLicense file. No input is required.

## License Server Configuration (CoLa Server)

The License server configuration is automatically filled based on the imported license file.

In case a Cola Server is not part of your license, you can manually fill the parameters and define external Cola Server. Please review the appropriate configuration.

Built-in

Server enabler: 2DBVD8NGPE8G8OV8

Primary license server IP\*:  ✓

Secondary license server IP:

Server port\*:  ✓

- Click on **Next**.

### 2.30.2.1.7 Configuring DICOM hosts

1. In the **DICOM Hosts** tab, the CT Console is configured as a DICOM host. Check the **Name** and the **Port**.

#### DICOM host configuration:

Please fill the information below about your DICOM host configuration.

Use the "Create host" button to create your DICOM Hosts and continue with the configuration.

##### Create new DICOM host:

Name*:	bay99	✓
Host name*:	bay99	✓
Application Entity Title*:	bay99	✓
IP address or domain name	192.168.101.1	✓
Port*:	4006	✓
Query/retrieve supported:	<input checked="" type="checkbox"/>	
Custom search:	<input type="checkbox"/>	
Encrypted (TLS)	<input type="checkbox"/>	

##### Created DICOM hosts:

bay99		

**Create host**

2. If the CT Console does not appear in the **Create DICOM hosts** list, click on **Create host**.
3. Click on **Next**.

### 2.30.2.1.8 Filling out the device information

- In the **Device Info** tab, check the prefilled information.

**Device Information**

Add device information

AWS System ID/AWS CRM number*:	262574CTMAXNANO	✓
Contract number:		
Global order number*:	TC06NAQAWS	✓
Install date*:	10/18/2022	<input type="button" value="Calendar"/> <input type="button" value="Delete"/>
Expiration date:		
Device description:		
Hospital name*:	AWBUC ENG LAB	
Address (line 1)*:	BUCK	
Address (line 2):		
City*:	BUCK	
State:		
Postal code:		
Country:	FR, France	
Other country:		
Address description:		
Service area:		
Service processor IP address:		

- Check the **AWS System ID / AWS CRM number**.

The AW Server System ID must be unique. It is built from the CT System ID by appending “NANO” at the end (for instance: 262474CTMAXNANO, where 262474CTMAX is the CT System ID).

**NOTE**

For the system connected via RSvP, the AW Server has a separate RSvP connection. As such, the AW Server System ID has been set as a “Child Asset” of the CT Console in some regions. Refer to the project manager for any help on the AW Server System ID.

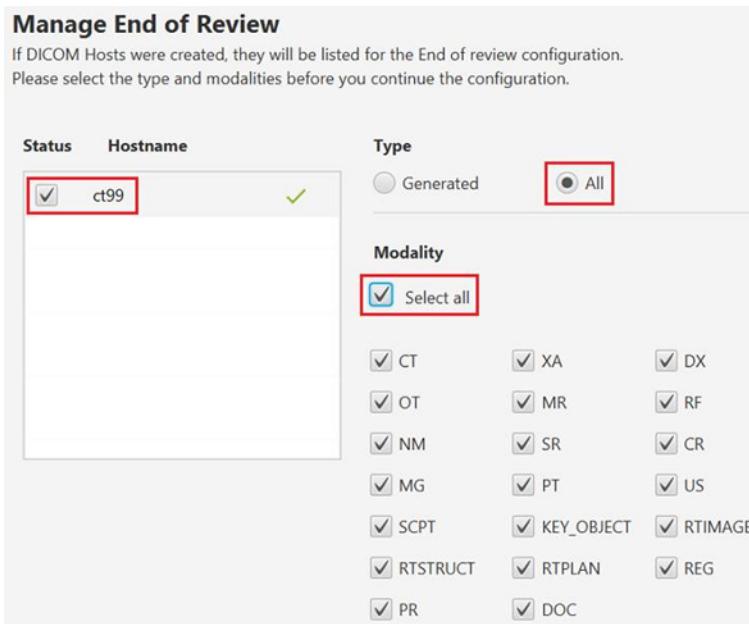
- If not already filled, fill in the **Global order number**, the **Hospital** name, the **Address (line 1)** and the **City** fields.
- Click on **Next**.

### 2.30.2.1.9 Configuring End of Review

The End of Review feature automatically sends processed images to the CT Console (configured as a DICOM Host), or to any other DICOM host, when exiting the application.

As the CT Console has been configured as a DICOM Host, the End of Review has been automatically configured.

- Check that CT Console DICOM host is selected, the **Type** is set to **All** and the **Select all** check box is selected in the **Modality** panel.



- Click on **Next**.

### 2.30.2.1.10 Summary

- In the **Summary** tab, review the configuration.

Use the scroll bar to review the settings from the previous sections.

#### Configuration Summary

Please review all the configuration information you can modify the parameters by going back to the appropriate page.

To export the configuration, please select one export option from the list according to your deployment mode.

After export you can start a new configuration or exit the application.

#### ▼ Network Configuration

Host name:	awsnano
Domain name:	Not filled
IP:	192.168.101.5
Network prefix:	24
Gateway:	192.168.101.1
DNS 1:	Not filled
DNS 2:	Not filled
MAC address:	52:54:00:17:a7:27
Time zone (Region/City):	Europe/Paris
NTP servers:	3.40.208.30

#### ▼ eLicenses

License ID:	0617a727
-------------	----------

- Click on **Next**.

### 2.30.2.1.11 Deploying the AW Server on a Virtual Machine

To finish the Virtual Machine creation and the AW Server deployment:

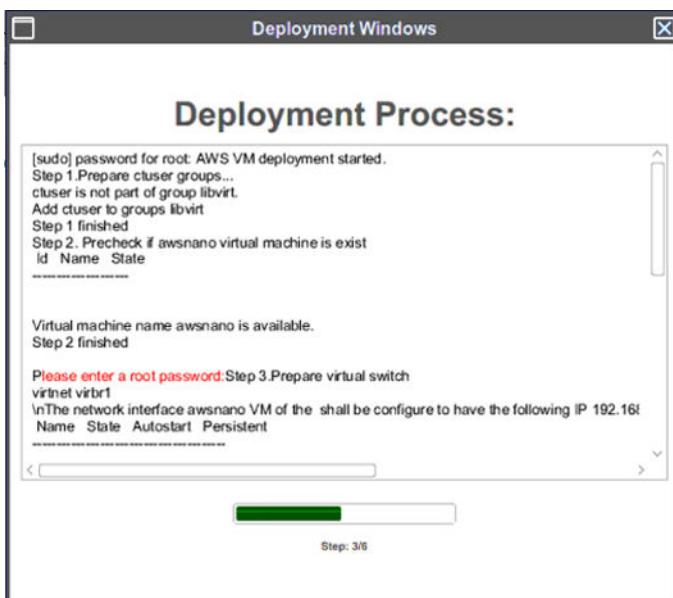
- In the **VM Deployment** tab, the **VM Name** and **Destination Folder** are prefilled.



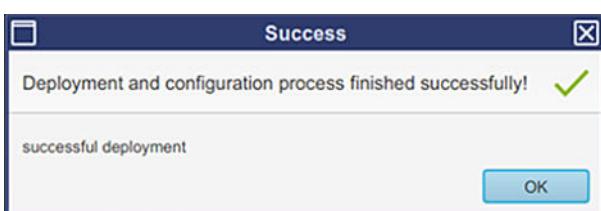
- Click on **Browse** and select the qcow2 iso file present in the /tmp/AWSUB directory.
- Enter the **CT OS Password of root user**.
- Click on **DEPLOY** to save the configuration and deploy the AW Server on a Virtual Machine.
- Click on **OK** in the popup that displays to actually start the AW Server deployment.



The **Deployment Process** window displays.



- When the **Success** popup displays, click on **OK** to close it.



- Click on **X** to close the **Deployment Process** window.
- Click on **X** to close the **AW Server Installation Tool** then, in the popup that displays, click on **Yes**.

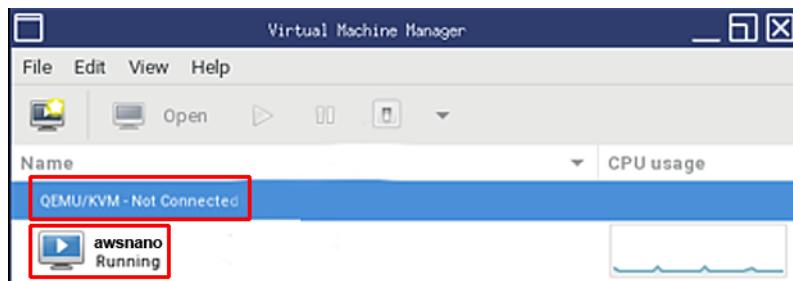
This completes the Virtual Machine creation with the AW Server deployment and the AW Server configuration.

### 2.30.2.2 Displaying the AW Server Console

The below steps described the process to display the AW Server Console from the CT Console.

1. In the Unix Shell (console/terminal) on the CT Console, login as **ctuser**, if not already done.
2. Type in the following command:

```
virt-manager <Enter>
```

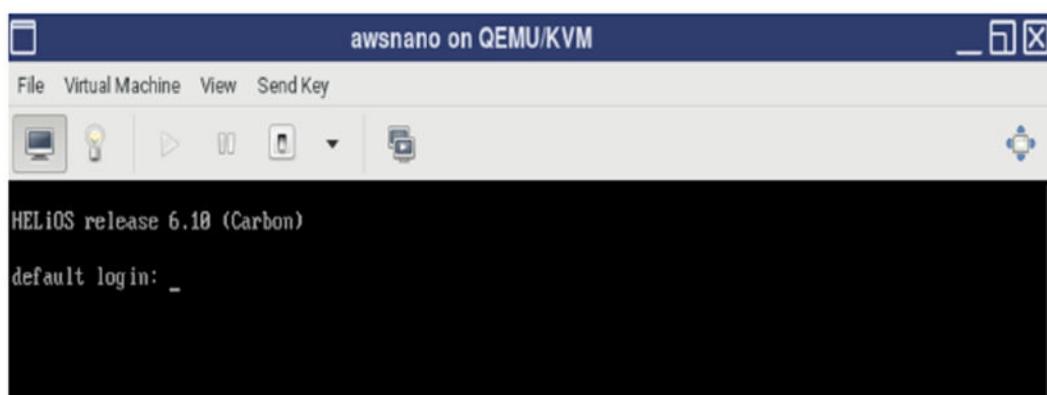


3. In the Virtual Machine Manager, double-click on **QEMU/KVM – Not Connected**.
4. Double-click on the **awsnano** Virtual Machine to open the AW Server Console.

The AW Server Console displays.

#### NOTE

The boot up process displays. If it remains a long time (roughly 5 min) in an intermediate state, press **<Enter>** to continue the boot up process.

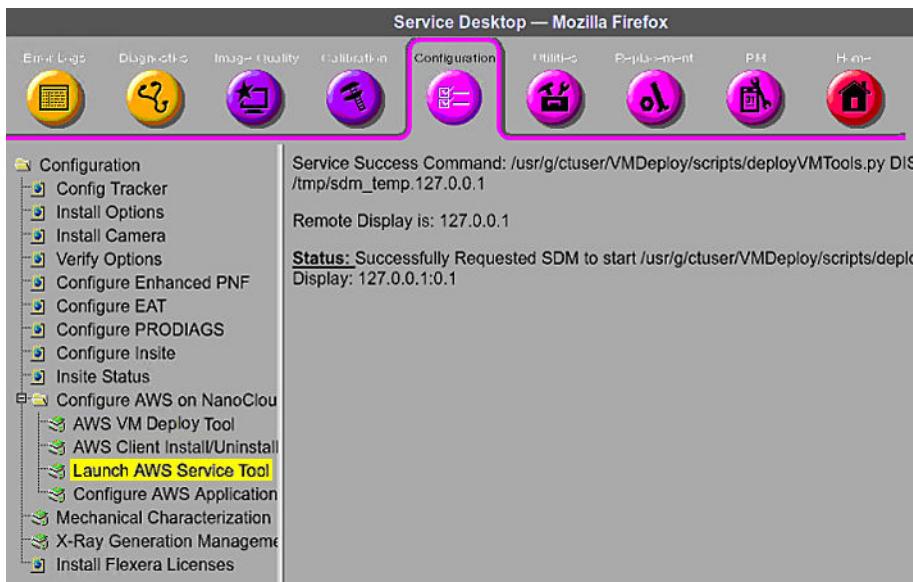


5. In the AW Server console, login as **root**.

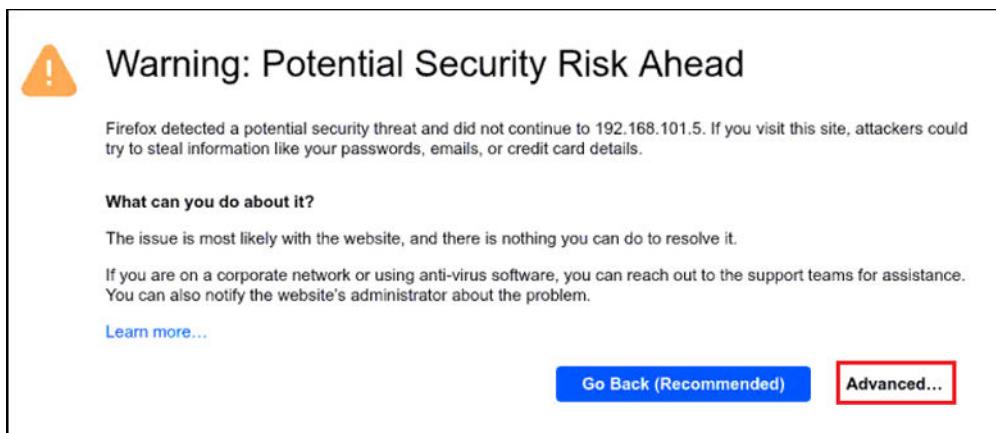
### 2.30.2.3 Launching Service Tools

The Service Tools allows to configure the AW Server.

- From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > Launch AWS Service Tools.**



- When launching the Service Tools, if the following window displays, select **Advanced...** then **Accept the risk and Continue.**



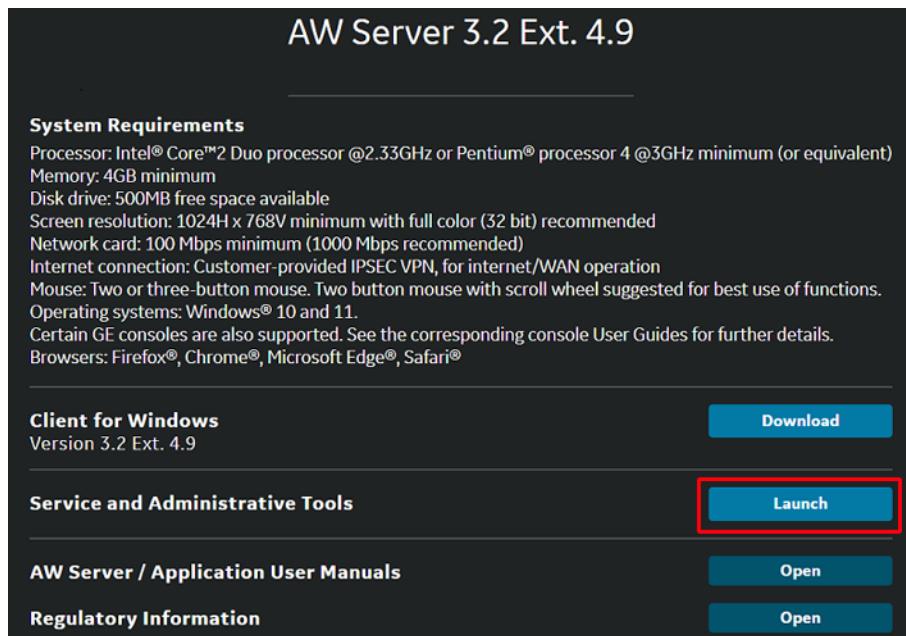
- Accept the cookies in the window that popups.

#### NOTE

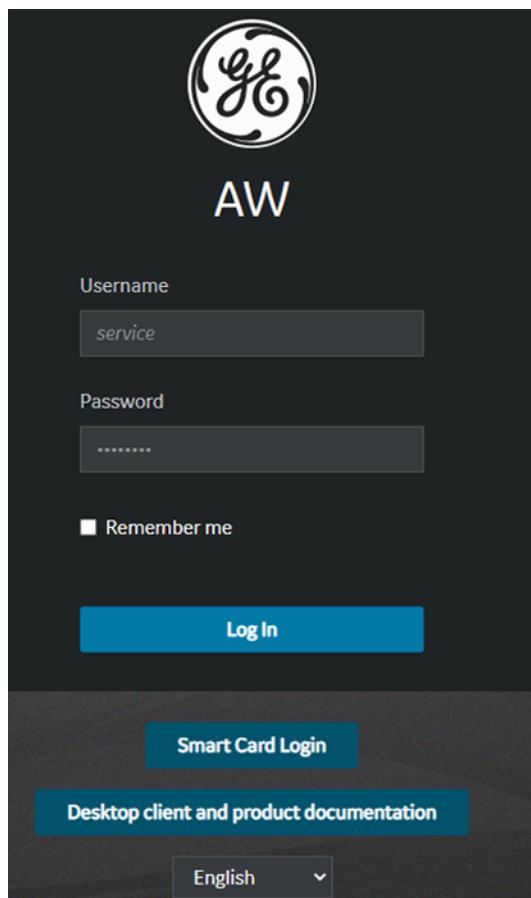
Depending on the Firefox version used, some features may not be available in the Service Tools. To remediate this issue, follow the below step:

- Open a new tab in Firefox and type in **about:config** to open the Firefox configuration page.
- Set **dom.moduleScripts.enabled** property's value to **false**.
- Close the tab.

- Click on the **Launch** button next to Service and Administrative Tools.



- The login screen appears.



- Login as service.

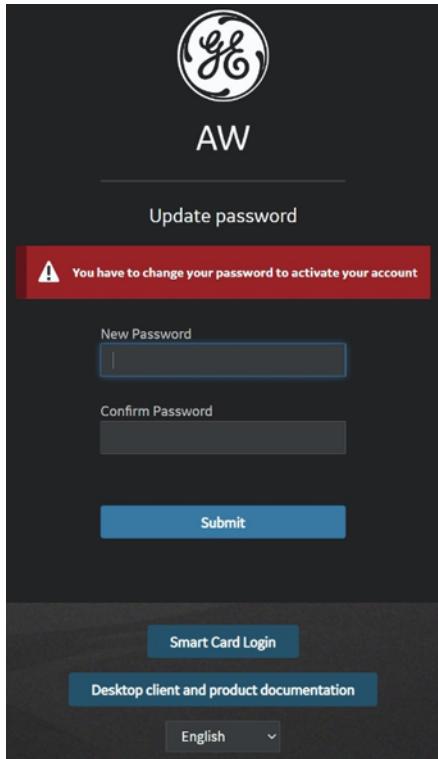
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

## NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.30.6.2 Changing the Passwords on page 434](#) for the password change guidelines.

7. The Service Tools opens with the installation/setup menus on the left.

The screenshot shows the Service Tools - AW Server interface. At the top, a message box states 'Maintenance is in progress since Oct 17, 2022, 2:28:33 PM' and lists several active tasks. Below this is a 'HealthPage' section with a table of system components and their statuses (CPU, Memory (RAM), Network Interface Controller, Storage, all marked as OK). There are 'Status Details' and 'Refresh' buttons. At the bottom, there is a 'System Configuration' table with three rows: System ID (CRM Number) BAY99\_AWS, Platform version aws-3.2-4.9-2241.4-b04b880e, and Hostname / IP Address bucaw70-239 / eth0: 3.249.70.239.

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

System Configuration	
System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.30.2.3.1 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, as shown below.

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.

**NOTE**

**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

### 2.30.2.4 Configuring the AW Server with the Service Tools

This section describes the configuration needed for the NanoCloud AW Server.

**NOTE**

As the AW Server has been configured using the AW Server Installation Tool, the AW Server has been mostly configured. Follow the below sections to complete the configuration.

#### 2.30.2.4.1 Setting up Remote Service

The below sections describe how to configure the AW Server for Remote Connectivity (GEHC only).

**NOTE**

For information, the RSvP model type for AW Server 3.2 is: AWS32\_RSVP.

**NOTE**

The AW Server has a separate RSvP connection. As such, the AW Server has a unique **System ID (CRM Number)**. Refer to the project manager for any help on the AW Server System ID.

### 2.30.2.4.1.1 RSvP Remote Service Setup

- From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration**.

The **Configure RSvP Agent** panel displays.

The screenshot shows the 'Configure RSvP Agent' interface with several sections:

- Overview:** A table showing agent status:

Agent	Status
Running	No
Connected	Unknown
Registered	Unknown
CRM Verified	Unknown
Quarantine	Unknown
Connection time	Unknown
- Configuration:** A table with configuration details:

Agent	Configuration
System ID (CRM Number) *	<AWS_SYSTEMID>
Serial Number *	<Mandatory>
Display Name	
Model Number *	AWS32_RSVP
Version	2.3
- Enterprise Server:** A table with enterprise server details:

Enterprise Server	Configuration
Hostname / IP *	insite.gehealthcare.com
Port Number *	443
- Proxy Server:** A table with proxy server details:

Proxy Server	Configuration
Hostname / IP	
Port Number	
- Mandatory fields:** A note indicating which fields are mandatory.
- Feature:** A table showing feature status:

Feature	Status
Prodiags	Enabled

2. Select the **Settings** tab.

Configure RSvP Agent		
Overview	Settings	Features
<b>Agent</b>	<b>Configuration</b>	
System ID (CRM Number) *	<AWS_SYSTEMID>	
Display Name		
<b>Enterprise Server</b>	<b>Configuration</b>	
Name	Production	
Hostname / IP *	insite.gehealthcare.com	
Port Number *	443	
<b>Proxy Server</b>	<b>Configuration</b>	
Hostname / IP	PITC-Zscaler-EMEA-Amster	
Port Number	80	
Username	*****	
Password	*****	
• Mandatory fields		
<input type="button" value="Refresh"/> <input style="background-color: #ff0000; color: white; border: 1px solid black; font-weight: bold;" type="button" value="Save"/> <input type="button" value="Restart"/>		

- In the **Agent** table, the **System ID (CRM NUMBER)** has been configured using the AW Server Installation Tool, check if the value is correct.  
Refer to [A.2 Specific field - Characters rules and limitations on page 555](#) for characters rules and limitations.
- In the **Enterprise Server** table, enter the **Name** of the RSvP server.

**NOTE**

There are two Enterprise Server, one in the US (e.g.: **Production**) and one in EU (e.g.: **Production-EU**). Use the one which is close to your location.

- In the **Proxy Server** table, if the customer use a Proxy:
  - Enter the **Hostname / IP** of the Proxy server.
  - Enter the **Port Number** of the Proxy server.
  - Enter the **Username** and **Password** of the Proxy server.

**NOTE**

This information can be acquired from the customer IT admin.

- Click on **Save** button to save the RSvP settings.

**NOTE**

Use the **Refresh** button to reset the settings to the previous values entered.

Use the **Restart** button to restart the RSvP Agent.

7. In the **Overview** tab, review the RSvP settings.

Agent	Configuration
System ID (CRM Number) *	<AWS_SYSTEMID>
Serial Number *	AWBUCLAB243_20210201_183831
Display Name	AWBUCLAB243-Test
Model Number *	AWS32_RSVP
Version	2.3
Enterprise Server	Configuration
Hostname / IP *	insite-eu.gehealthcare.com
Port Number *	443
Proxy Server	Configuration
Hostname / IP	PITC-Zscaler-EMEA-Amsterdam3PR.proxy.corporate.ge.com
Port Number	80
* Mandatory fields	

8. Click on **Start** button to start the RSvP Agent.

The **Running** status turns green.

Agent	Status
Running	Yes
Connected	No
Registered	No
CRM Verified	No
Quarantine	No
Connection time	N/A

#### NOTE

Use the **Stop** button to stop the RSvP Agent.

Use the **Restart** button to restart the RSvP Agent.

9. Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green (except for the **CRM Verified** status - see [2.30.2.4.1.2 System ID \(CRM Number\) verification on page 398](#)).

#### NOTE

Do not hesitate to select the **Refresh** button again till the status turns green (see below status definition and latency to turn green).

Agent	Status
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	No
Quarantine	No
Connection time	Mon 1 Feb 2021 06:43:30 PM GMT+1

Status definition:

- **Running:** Value is **Yes** if the Agent is running. Otherwise, the value is **No**.
- **Connected:** Value is **Yes** if the Agent can be registered to the back office and is actively polling the back office. If the Agent is unable to successfully poll the back office, the value is **No**.
- **Registered:** Value is **Yes** if the Agent has successfully registered with the back office and has received confirmation of this registration. Otherwise, the value is **No**.

This value does not reflect if the Agent is actively polling. It is a 1 time notification of successful registration.

To see if the Agent is currently communicating with back office, see the **Connected** status.

#### **NOTE**

The **Yes** status may take a minute or two to appear.

- **CRM Verified:** If the value is **Yes**, it means that the System ID (a.k.a. CRM Number) is in CRM systems. Otherwise, the value is **No** (see [2.30.2.4.1.2 System ID \(CRM Number\) verification on 398](#)).

#### **NOTE**

The **Yes** status may take up to 5 minutes to appear.

- **Quarantine:** Value is **Yes** if the Agent is currently in Quarantine. Otherwise, the value is **No**. If Agent status returns quarantine values as **Yes**, it means that RSvP back office cannot uniquely identify the device as some other device is also running an agent using the same System ID (CRM Number).

#### **NOTE**

The FE shall contact the RSvP team to resolve the issue.

- **Connection time:** Value is the last successful connection date/time of the RSvP Agent with the back office.

#### **NOTE**

The RSvP status is also displayed in the **Remote Service** table of the Healthpage.

## **2.30.2.4.1.2 System ID (CRM Number) verification**

#### **NOTICE**

It is important to have the System ID (CRM Number) verified now, so that the system will be able to upload its configuration to the AWCCT website and automatically receive in return the Registration Configuration key, necessary to enable the AW Server.

#### **NOTE**

Registration will have to be done manually if RSvP is not available.

#### **NOTE**

Without the Registration key, the AW Server will not allow exiting from the Maintenance mode and therefore be accessible to the Clients.

1. From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice) Configuration**, check that the status of the RSvP Agent are green.

Agent	Status
Running	Yes
Connected	Yes
Registered	Yes
CRM Verified	Yes
Quarantine	No
Connection time	Mon 1 Feb 2021 07:46:44 PM GMT+1

2. If the **CRM Verified** status remains red, select the **Refresh** button to refresh the RSvP Agent status.

As mentioned in previous section, the **CRM Verified** status takes time to turn green.

If it remains red after 5 minutes, contact the local RSvP team to get the System ID (CRM Number) verified for the system.

When all the RSvP Agent status are green, the system is ready to be accessed remotely.

3. Proceed to the connection tests with FFA, to make sure the system is ready to be accessed remotely.

## 2.30.3 AW Server Upgrade

### Important

Follow this section only for an **upgrade** of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to upgrade, deploy and configure the NanoCloud AW Server.

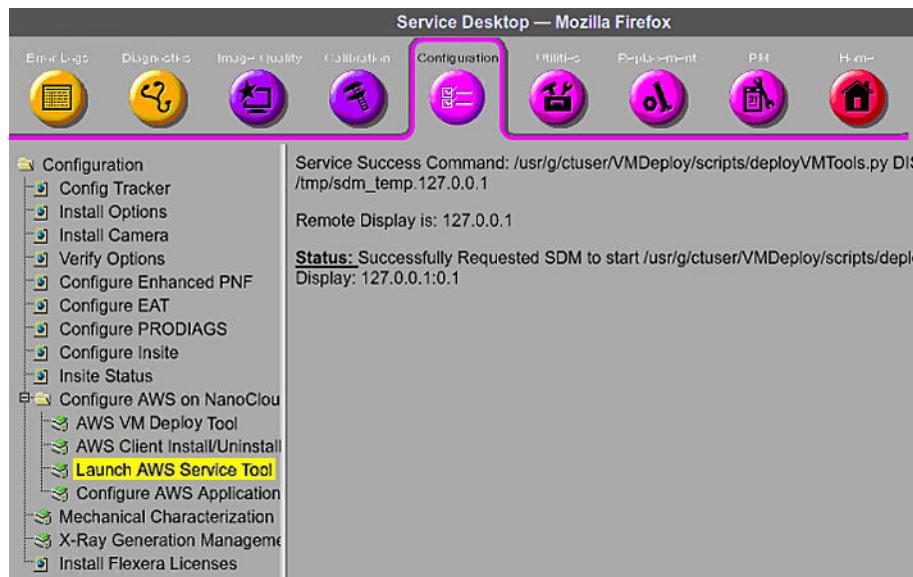
### 2.30.3.1 Launching Service Tools

#### NOTE

If the Service Tools is already launched, skip this section.

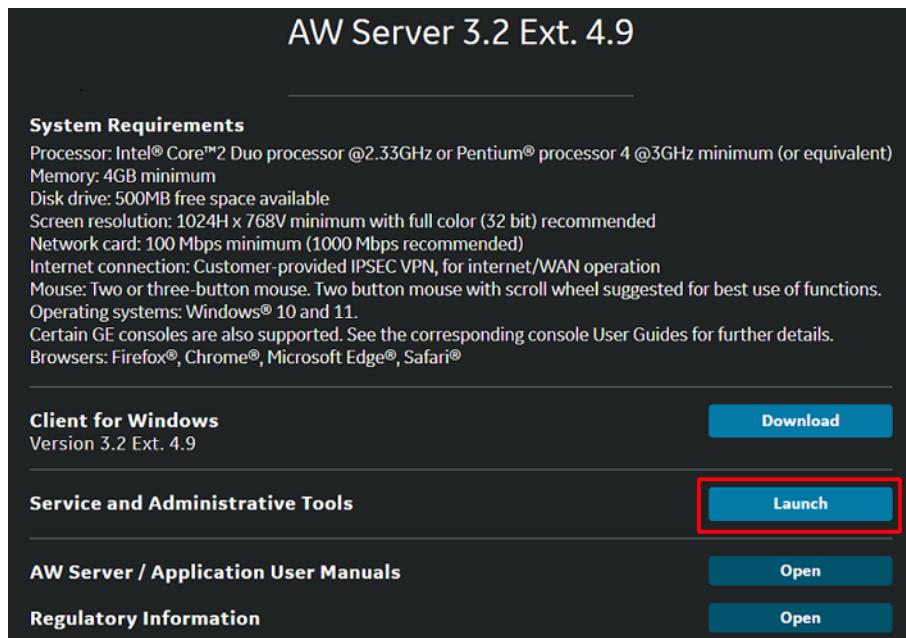
The Service Tools allows to configure the AW Server.

1. Start the Service Desktop interface using the CSD tool:

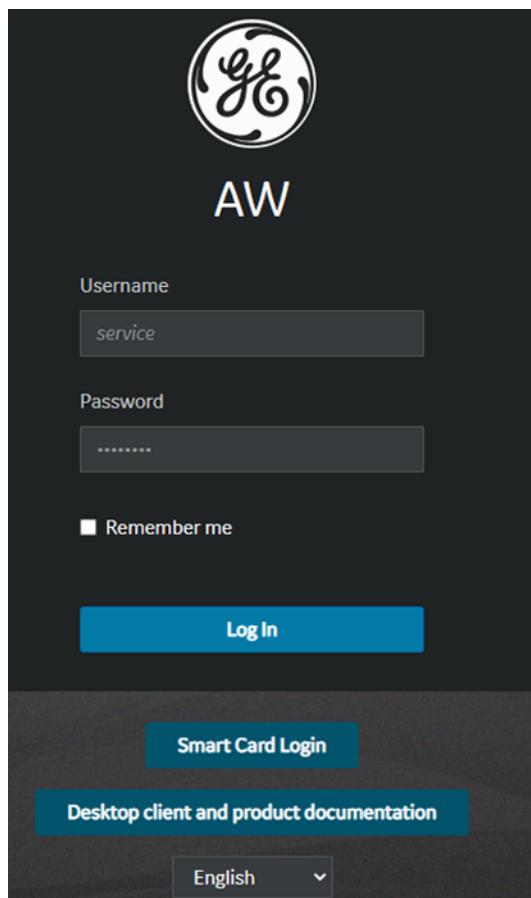


2. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > Launch AWS Service Tools**.
3. Accept the cookies in the window that popups.

- Click on the **Launch** button next to Service and Administrative Tools.



- The login screen appears.



- Login as service.

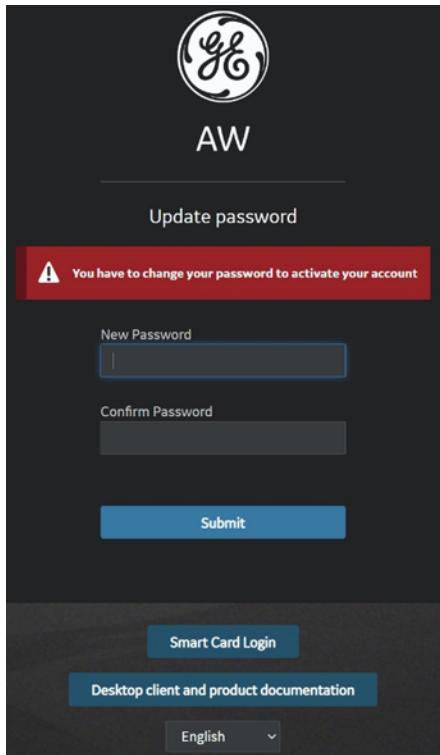
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

## NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.30.6.2 Changing the Passwords on page 434](#) for the password change guidelines.

- The Service Tools opens with the installation/setup menus on the left.

 A screenshot of the Service Tools - AW Server interface. The top bar shows the title 'CST (3.2-4.9-b04b880e) - AW Server ST (3.2-4.9-b04b880e) [service]' and a 'Logout' link. A prominent red banner at the top right states 'Maintenance is in progress' since Oct 17, 2022, 2:28:33 PM. It lists several tasks: 'Global Installed Base data is not sent yet to GEI', 'New package is available. Click here for details.', 'Remote Service (RSvP) is not properly configured or not running. Click here for details.', 'Last password generation and synchronization failed on Oct 30, 2022, 2:00:01 AM Click here for details.', and 'Change all default passwords after installation!'. On the left is a navigation menu with links like 'HealthPage', 'Initial configuration', 'Administrative', etc. The main area features a 'HealthPage' section with a table of system status (CPU, Memory, Network Interface Controller, Storage) and buttons for 'Status Details' and 'Refresh'. Below that is a 'System Configuration' table with rows for System ID, Platform version, and Hostname / IP Address.
 

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

System Configuration	
System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.30.3.1.1 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, as shown below.

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.

**NOTE**

**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

### 2.30.3.2 Entering the Maintenance Mode

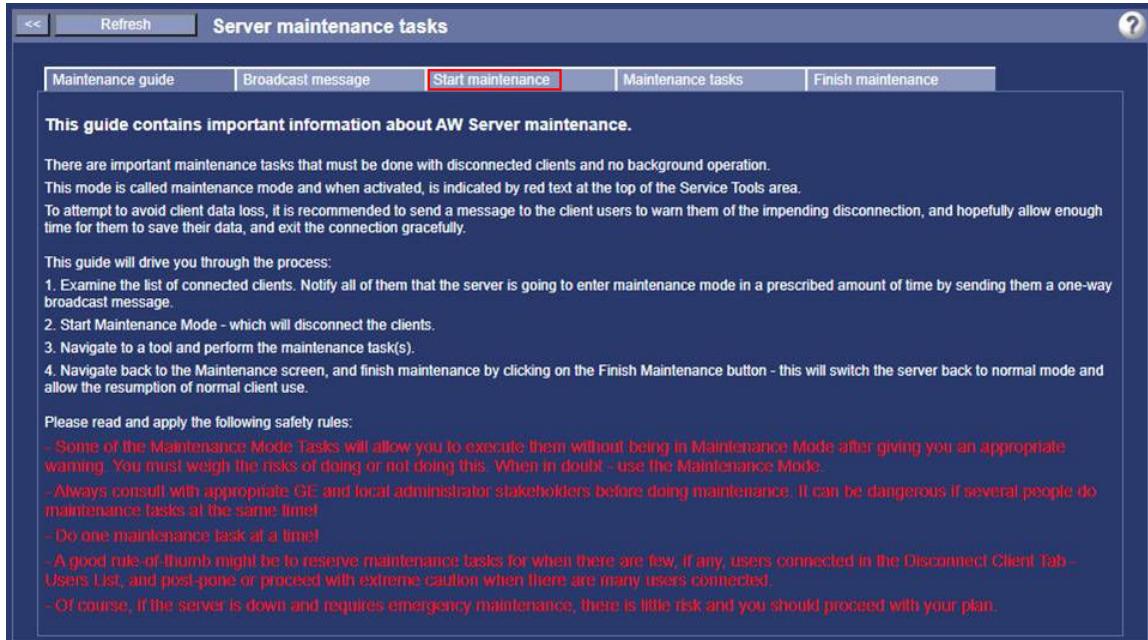
**NOTE**

If the AW Server is already in Maintenance Mode, skip this section.

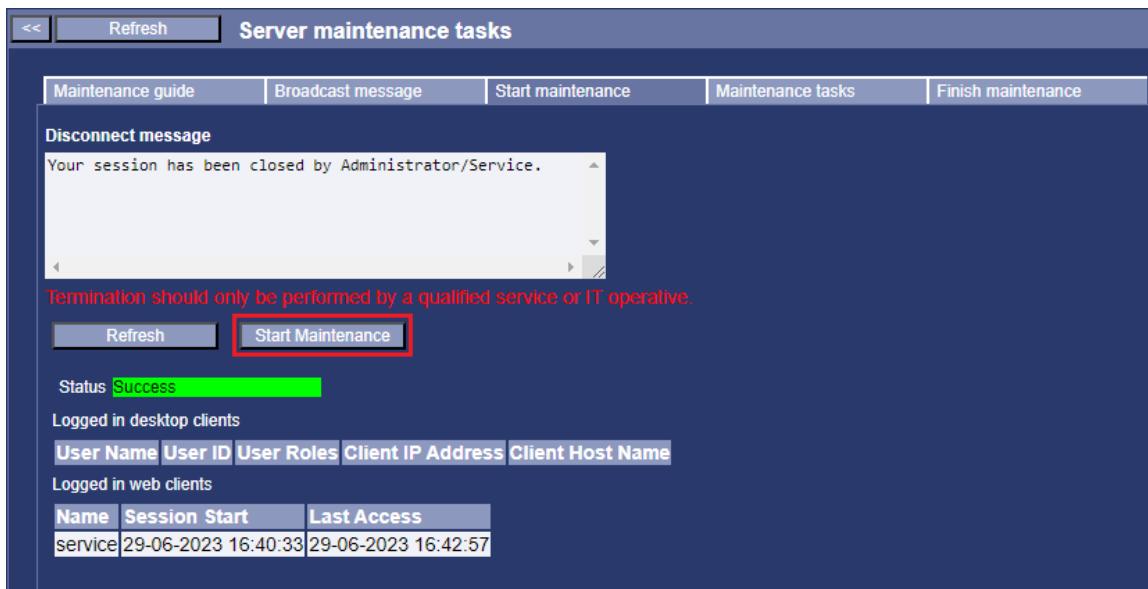
The Maintenance Mode allows the AW Server to be "isolated" from the AW Server Clients in order to perform maintenance operations such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters ...

Follow the below steps to place the AW Server in Maintenance Mode:

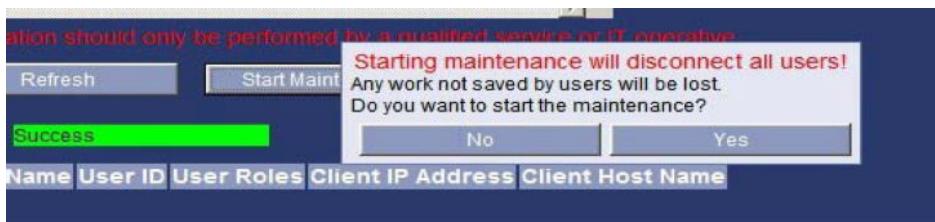
- From the Service Tools, select **Maintenance > Maintenance** and select the **Start maintenance** tab.



- Click on the **Start Maintenance** button to start the Maintenance Mode:



A pop-up confirmation message appears.



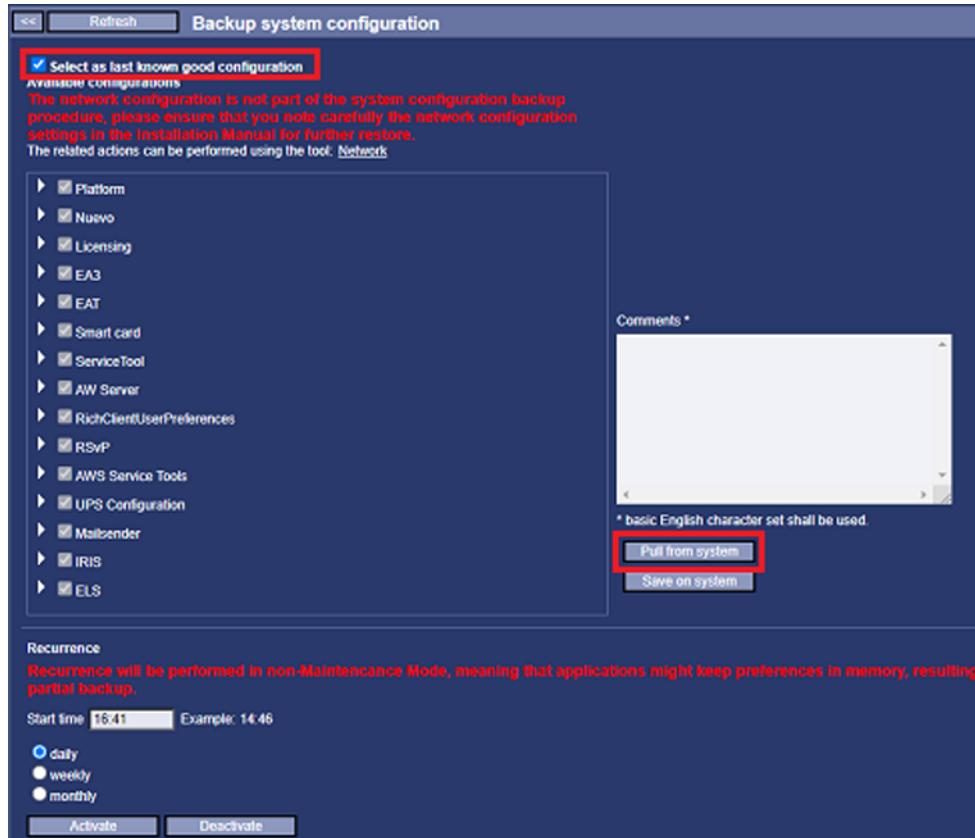
- Click on **Yes**.

Another pop-up states that you are in maintenance mode. And the Maintenance is in progress banner will display at the top of the Service Tools.

The screenshot shows the 'Service Tools - AW Server' interface. At the top, it says 'CST (3.2-3.2-975c1d6d) - AW Server ST (3.2-3.2-975c1d6d) [service]'. In the center, a red box highlights the message 'Maintenance is in progress since Jan 21, 2019, 6:14:11 PM' and 'Active Service Tools tasks: 0'. Below that, it says '• Global Installed Base data is not sent yet to GE!'. On the right, there's a 'Logout' link.

### 2.30.3.3 Backing up the configuration

- From the Service Tools, select **Maintenance > Backup > System configuration**.



- Check the **Select as last known good configuration** radio button.
- Keep everything selected and click on **Pull from system** to save the configuration in the `/usr/g/ctuser/Downloads` directory.

### 2.30.3.4 Preparing and deploying the AW Server with the AW Server Installation Tool

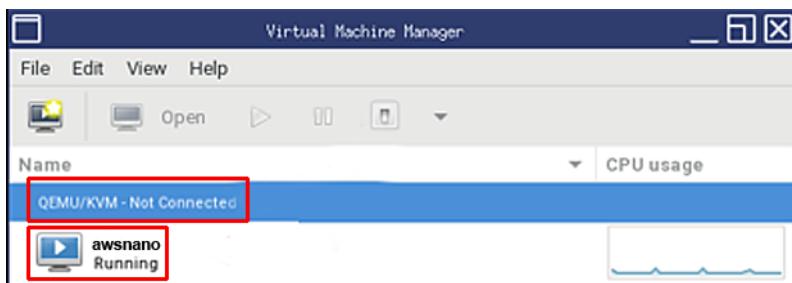
The AW Server Installation Tool allows to prepare and perform the basic AW Server configuration. It generates a configuration file that can be interpreted by the AW Server to perform the configuration automatically during its first start. The Installation Tool allows then to deploy the AW Server in a Virtual Machine of the CT Console.

#### 2.30.3.4.1 Shut down the Virtual Machine

- In the Unix Shell (console/terminal) on the CT Console, login as **ctuser**, if not already done.
- Display the Virtual Machine Manager:

Type the following command in the CT Console terminal:

```
virt-manager <Enter>
```



3. In the Virtual Machine Manager, double-click on **QEMU/KVM - Not Connected** and select the **awsnano** virtual machine.
4. Shut down the Virtual Machine:

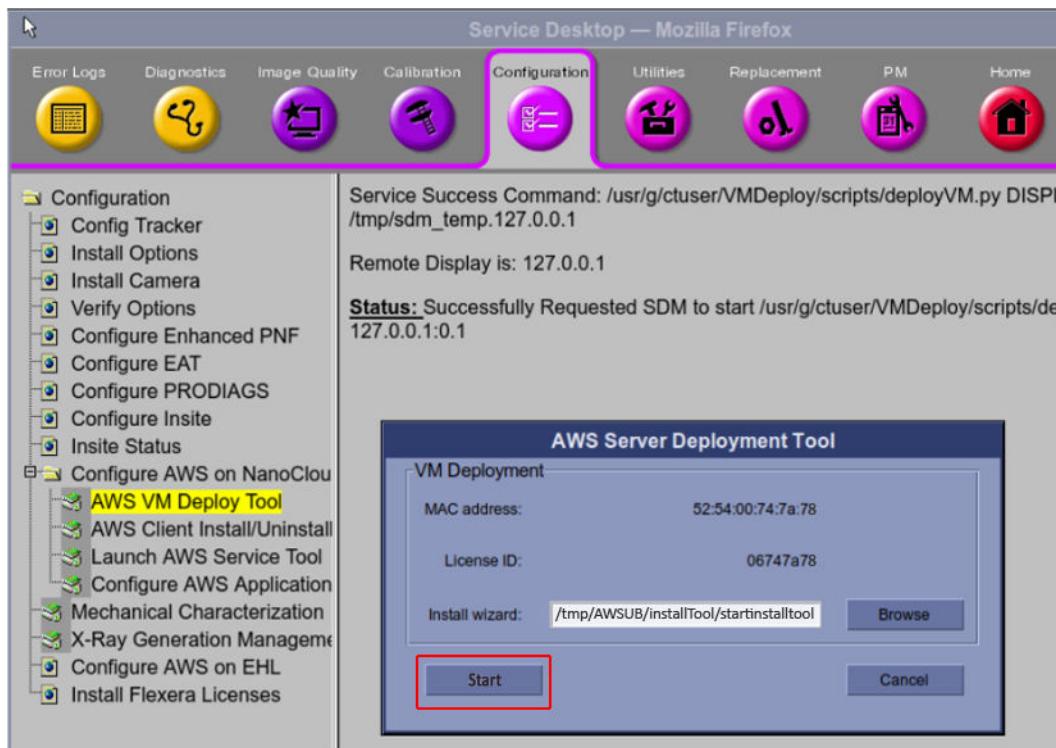


Make sure the Virtual Machine is stopped. If not, right click the Virtual Machine and select **Shut Down / Shut Down or Force Off**.

#### 2.30.3.4.2 Launching the AW Server Installation Tool

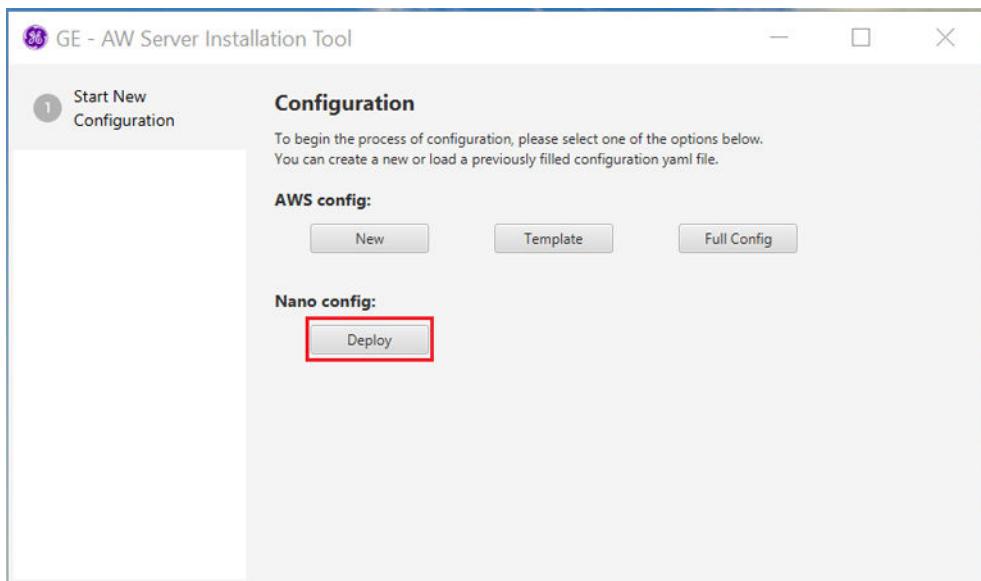
1. Insert the USB media into the CT Console.
2. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > AWS VM Deploy Tool**.

The **AWS Server Deployment Tool** window displays.

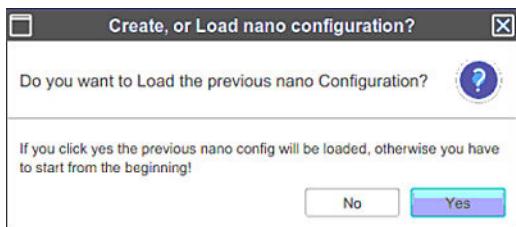


3. Click on **Start** button.

The AW Server Installation Tool appears.

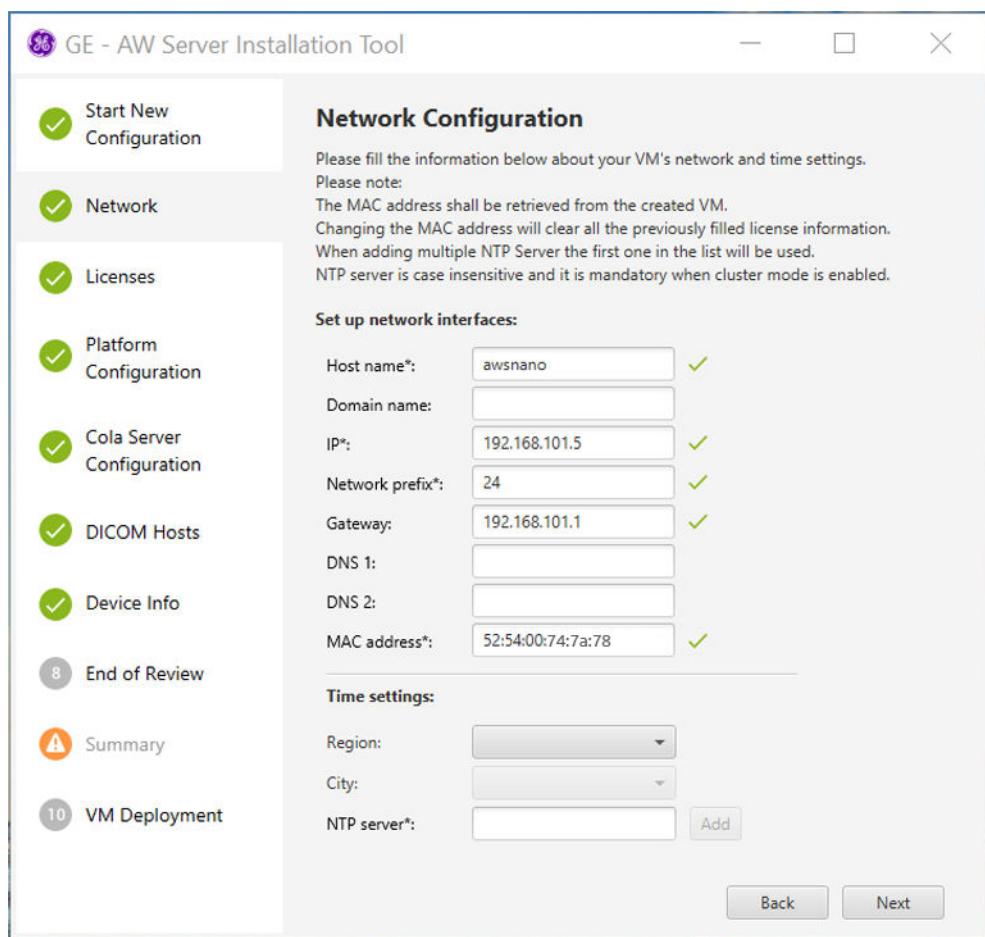


4. In the **Start New Configuration** tab, click on **Deploy**.



5. In the **Create, or Load nano Configuration ?** popup, click on **Yes**.

The **AW Server Installation Tool** displays the different tabs used to configure the AW Server and move to the **Network** tab.



### 2.30.3.4.3 AW Server Installation Tool navigation and Field Filling Rules

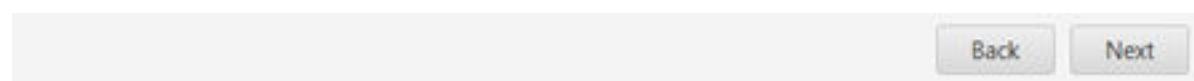
In the following steps all fields marked with an asterisk (\*) are mandatory and must be filled out. Other fields are optional.

If a field is wrongly filled, the symbol appears next to the field and also on the corresponding tab and the *Summary* tab, as shown in the example below.

When all the mandatory fields are correctly filled, a green check appears near the fields and on the tab, as shown in the example below:

 <b>Network</b>	<b>Set up network interfaces:</b> Host name*: awsnano ✓ Domain name:  IP*: 192.168.1015  Network prefix*: 24 ✓	 <b>Network</b>	<b>Set up network interfaces:</b> Host name*: awsnano ✓ Domain name: IP*: 192.168.101.5 ✓ Network prefix*: 24 ✓
3 <b>Licenses</b>			4 <b>Platform Configuration</b>
Field wrongly filled (here the IP field)	Field correctly filled		

To navigate through the tabs click directly on the tab or on the **Next** and/or **Back** buttons at the bottom right of the Installation Tool.



#### NOTE

Refer to [A.2 Specific field - Characters rules and limitations on page 555](#), to know the characters rules and limitations of the specific fields (Hostname, AE Title, IP Address, Port, System ID, Label/Name).

### 2.30.3.4.4 Configuring the AW Server with the Installation Tool

Verify the fields from the tabs listed below:

1. In the **Network** tab, check the **Host name**, the IP address, the **Network prefix**, the **Default Gateway** and the **MAC address**.

2. Click on **Next**.

In the **Licenses** tab, the licenses are uploaded.

3. Click on **Next**.

In the **Platform Configuration** tab, the Platform Integration Mode is filled based on the imported eLicense file.

4. Click on **Next**.

In the **Cola Server Configuration** tab, the License Server configuration is filled based on the imported eLicense file.

5. Click on **Next**.

In the **DICOM Hosts** tab, the CT Console is configured as a DICOM host.

6. Click on **Next**.

7. In the **Device Info** tab, check the information.

The AW Server System ID must be unique. It is built from the CT System ID by appending *NANO* at the end (for instance: 262474CTMAXNANO, where 262474CTMAX is the CT System ID).

#### NOTE

For the system connected via RSvP, the AW Server has a separate RSvP connection.

As such, the AW Server System ID has been set as a "Child Asset" of the CT Console System ID, in some regions. Refer to the project manager for any help on the AW Server System ID.

8. Click on **Next**.

In the **End of Review** tab, the CT Console DICOM host is selected.

9. Click on **Next**.

10. In the **Summary** tab, review the configuration.

Use the scroll bar to review the settings from the previous sections.

11. Click on **Next**.

### 2.30.3.4.5 Deploying the AW Server on the Virtual Machine

To finish the Virtual Machine upgrade and the AW Server deployment:

1. In the **VM Deployment** tab, the **VM Name** and **Destination Folder** are prefilled.

**VM Deployment**

The next step of the installation process is the Virtual Machine Deployment. It will take some minutes...

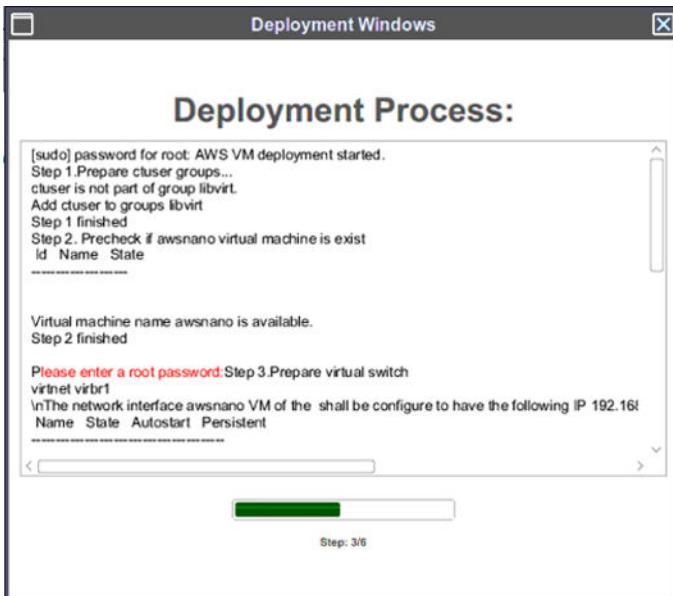
VM Name*:	awsnano	✓
Image source*:	/tmp/AWSUB/aws-3.2-4.9-0.qcow2.iso	✓
Browse		✓
Destination Folder*:	/usr/g/ctuser/AWSVM	✓
CT OS password of root user*:	*****	✓
<b>DEPLOY</b>		

2. Click on **Browse** and select the latest qcow2 iso file present in the /tmp/AWSUB directory.

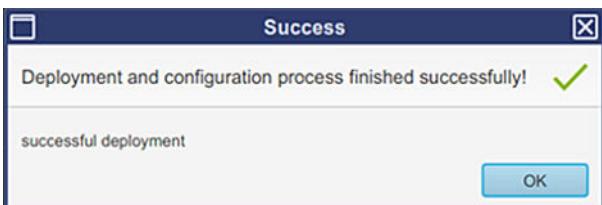
3. Enter the **CT OS password of root user**.
4. Click on **DEPLOY** to save the configuration and deploy the AW Server on a Virtual Machine.
5. Click on **OK** in the popup that displays to actually start the AW Server deployment.



The **Deployment Process** window displays.



6. When the **Success** popup displays, click on **OK** to close it.



7. Click on **X** to close the **Deployment Process** window.
8. Click on **X** in the **AW Server Installation Tool** then, in the popup that displays, click on **Yes** to exit the Installation Tool.

This completes the Virtual Machine upgrade with the AW Server deployment and the AW Server configuration.

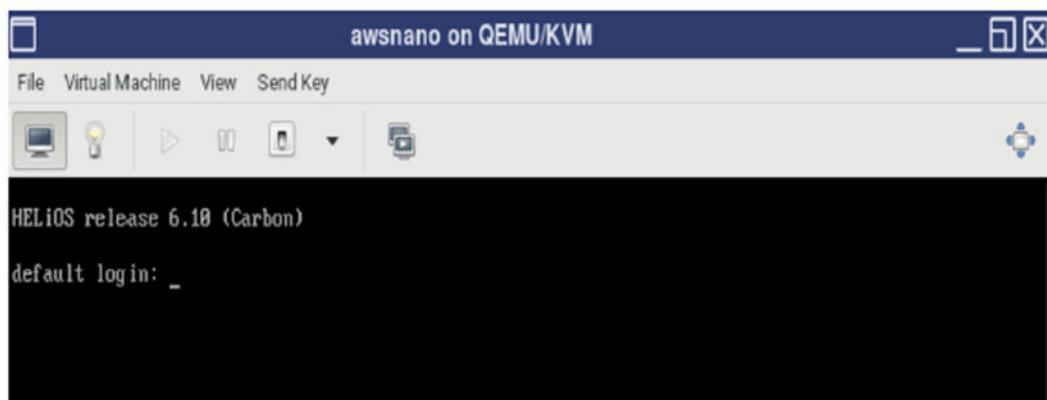
### 2.30.3.5 Displaying the AW Server Console

The below steps described the process to display the AW Server Console from the CT Console.

1. In the Virtual Machine Manager, double-click on the **awsnano** Virtual Machine to open the AW Server Console.

#### **NOTE**

The boot up process displays. If it remains a long time (roughly 5 min) in an intermediate state, press **<Enter>** to continue the boot up process.

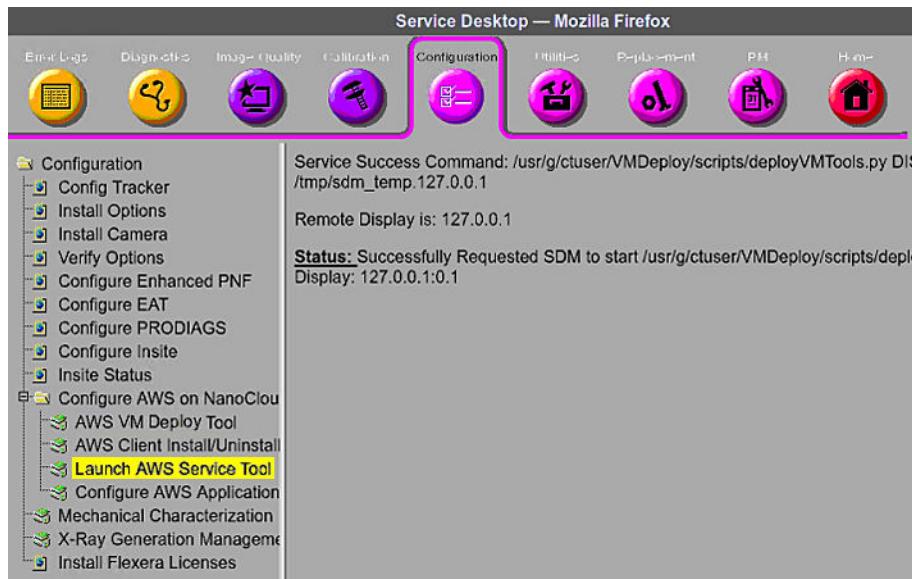


2. In the AW Server console, login as **root**.

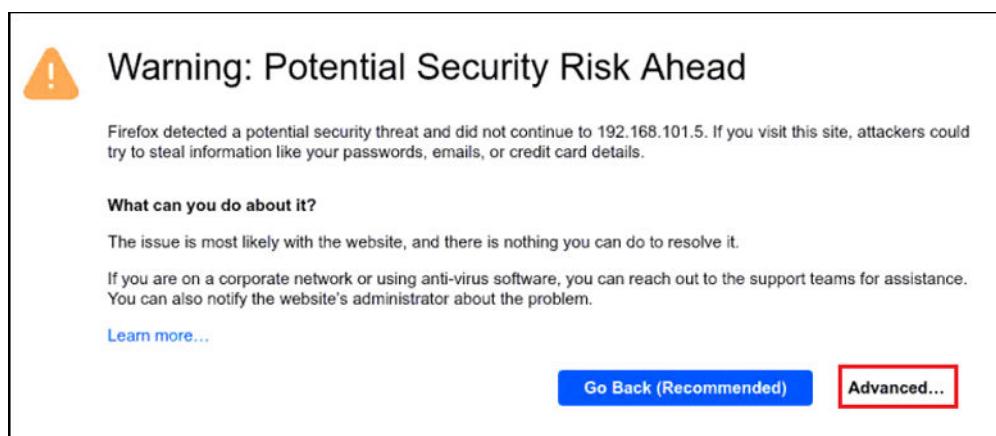
### 2.30.3.6 Launching Service Tools

The Service Tools allows to configure the AW Server.

1. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > Launch AWS Service Tools**.



2. When launching the Service Tools, if the following window displays, select **Advanced...** then **Accept the risk and Continue**.

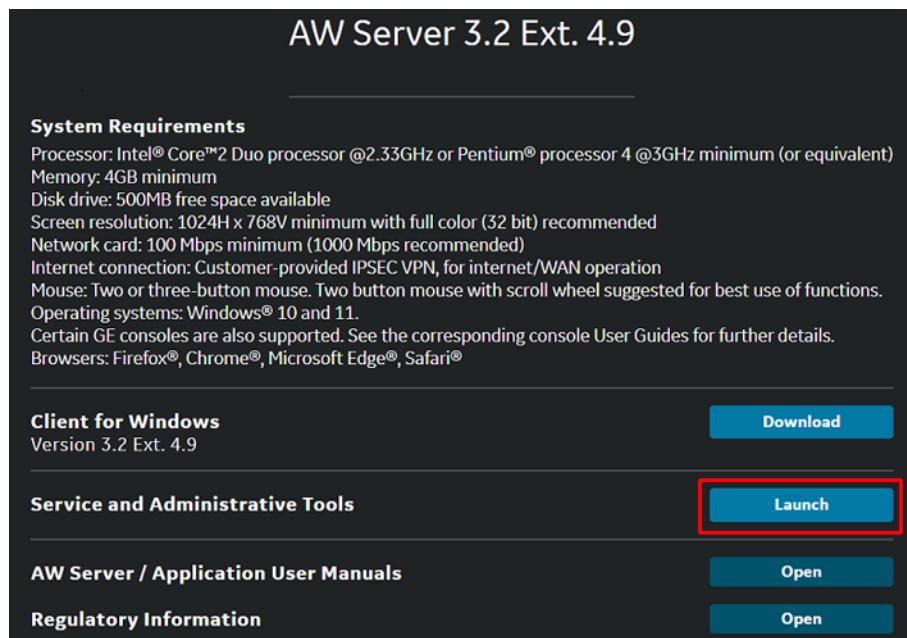


3. Accept the cookies in the window that popups.

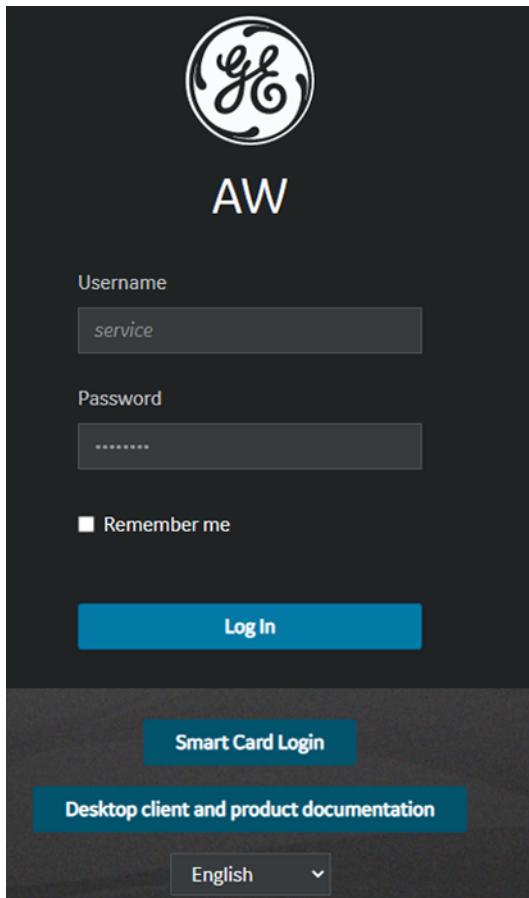
**NOTE**

Depending on the Firefox version used, some features may not be available in the Service Tools. To remediate this issue, follow the below step:

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.
4. Click on the **Launch** button next to Service and Administrative Tools.



5. The login screen appears.



6. Login as **service**.

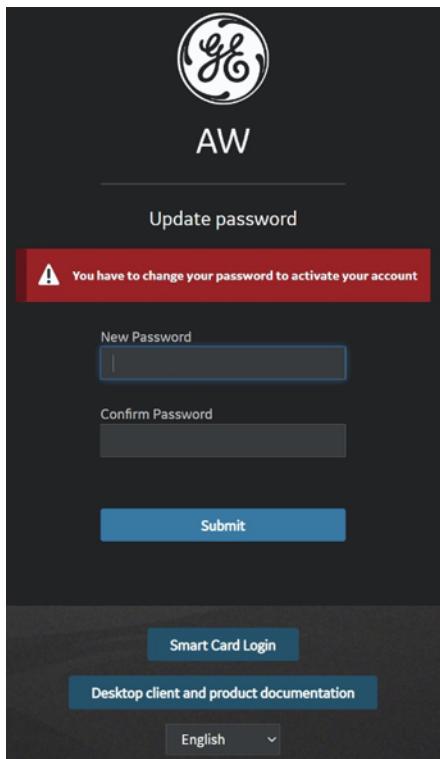
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

**NOTICE**

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.30.6.2 Changing the Passwords on page 434](#) for the password change guidelines.

- The Service Tools opens with the installation/setup menus on the left.

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

System Configuration	
System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

#### NOTE

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.30.3.7 Restoring the saved configuration

- From the Service Tools, select **Maintenance > Restore > System configuration**.
- Upload the configuration file previously saved in the `/usr/g/ctuser/Downloads` directory or an USB media.
  - Select **Upload**.

b. Click on **Upload configuration**.

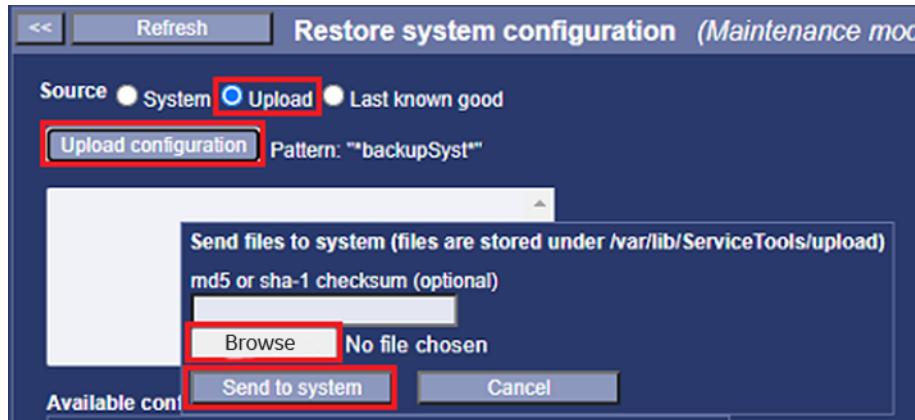
A pop-up window appears.

c. Click on **Browse**.

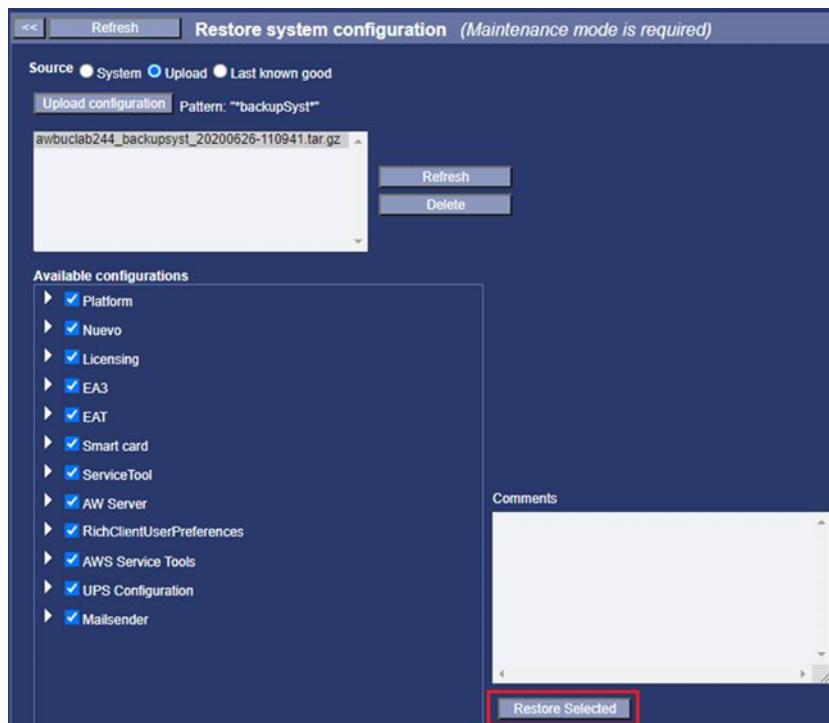
d. Choose the configuration file to upload and click on **Send to system**.

When the upload is complete, a pop-up window appears.

e. Click on **OK**.



3. Select the configuration previously uploaded, then click on **Restore Selected**.

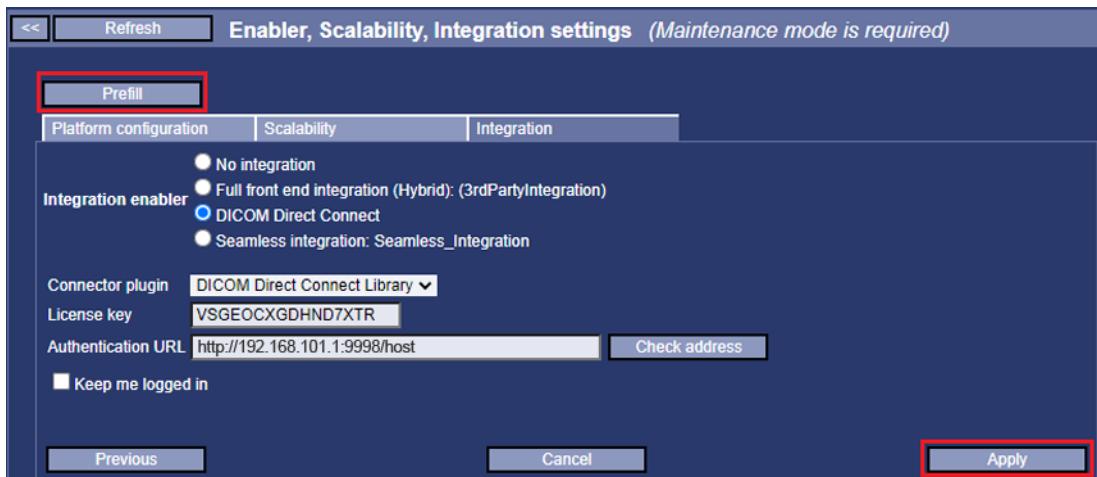


### 2.30.3.8 Restoring the integration

The Platform configuration has been restored. However, it needs to be applied to be effective:

1. From the Service Tools, select **Initial configuration > Platform Configuration**.
2. Check that the **Platform license Key** displays.

- Click on **Next** twice to display the **Integration** tab.



- Click on the **Prefill** button to populate the integration parameters.

#### NOTE

If the integration parameters do not populate, enter them manually.

- Click on **Apply** to apply the platform configuration.

Acknowledge the confirmation popups that display.

The AW Server reboot will be done later.

### 2.30.3.9 Restarting the RSvP Agent

The Remote Connectivity has been restored (GEHC only). However, the RSvP Agent needs to be restarted.

- From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice)**.



- Click on the **Restart** button to restart the RSvP Agent.
- Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green.

### 2.30.4 AW Server Service Pack Installation

#### Important

Follow this section **only** for the **installation of patches** (Service Pack) on top of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to install the Service Packs on top of the current AW Server release. 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**

For the systems connected via RSvP, if a new version of an AW Server Service Pack is available, it has been loaded onto the AW Server (from the software delivery portal).

#### **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.

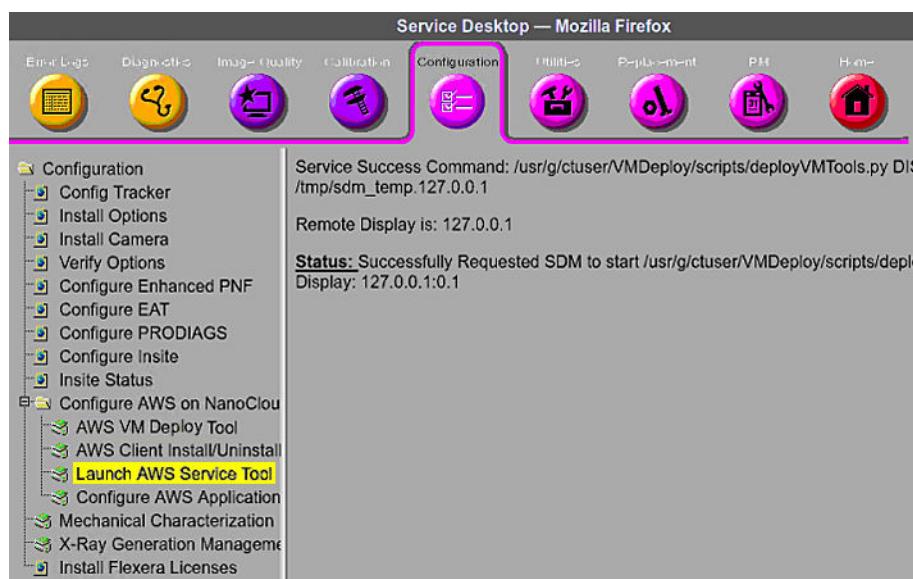
### **2.30.4.1 Launching Service Tools**

#### **NOTE**

If the Service Tools is already launched, skip this section.

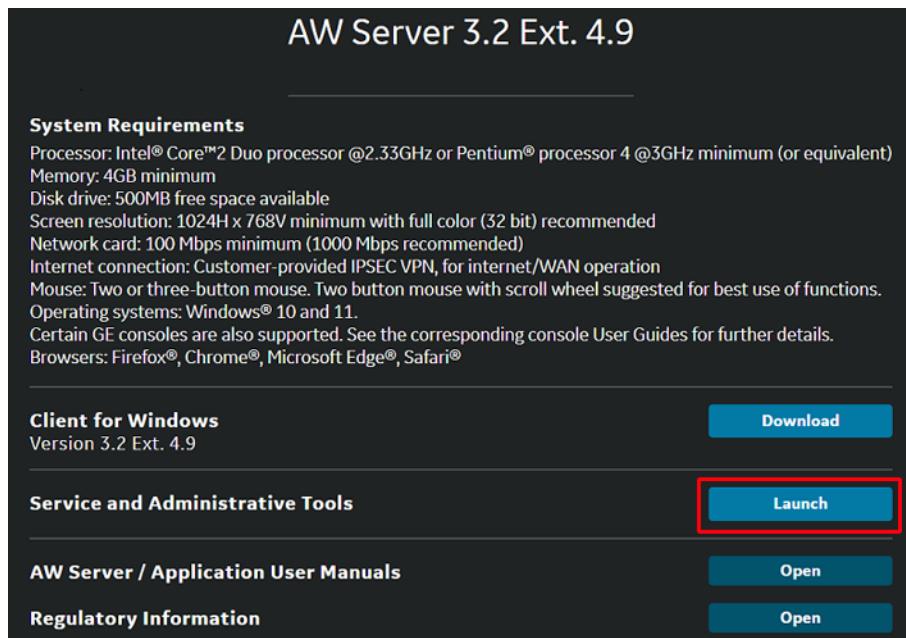
The Service Tools allows to configure the AW Server.

1. Start the Service Desktop interface using the CSD tool:

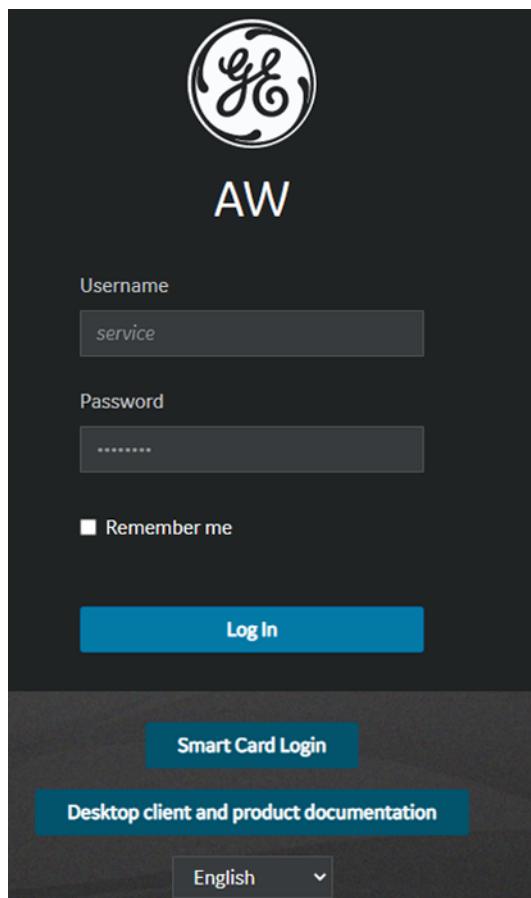


2. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > Launch AWS Service Tools**.
3. Accept the cookies in the window that popups.

- Click on the **Launch** button next to Service and Administrative Tools.



- The login screen appears.



- Login as service.

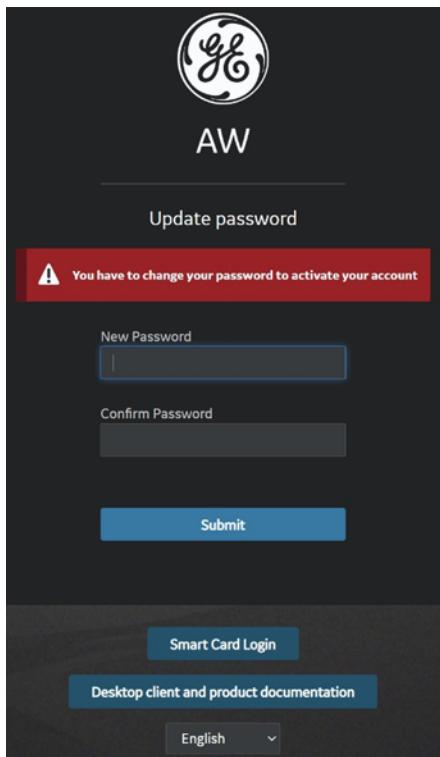
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

## NOTICE

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.30.6.2 Changing the Passwords on page 434](#) for the password change guidelines.

7. The Service Tools opens with the installation/setup menus on the left.

The screenshot shows the "Service Tools - AW Server" interface. At the top, a red banner displays "Maintenance is in progress" since Oct 17, 2022, 2:28:33 PM. It lists several tasks: "Global Installed Base data is not sent yet to GEI", "New package is available. Click here for details.", "Remote Service (RSvP) is not properly configured or not running. Click here for details.", "Last password generation and synchronization failed on Oct 30, 2022, 2:00:01 AM Click here for details.", and "Change all default passwords after installation!". Below this is a "HealthPage" section with tabs for "Virtual Machine" and "Status". The "Virtual Machine" table shows four items: CPU (OK), Memory (RAM) (OK), Network Interface Controller (OK), and Storage (OK). There are "Status Details" and "Refresh" buttons. At the bottom is a "System Configuration" table with three rows: System ID (CRM Number) BAY99\_AWS, Platform version aws-3.2-4.9-2241.4-b04b880e, and Hostname / IP Address bucaw70-239 / eth0: 3.249.70.239.

**NOTE**

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.30.4.1.1 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, as shown below.

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.

**NOTE**

**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

### 2.30.4.2 Entering the Maintenance Mode

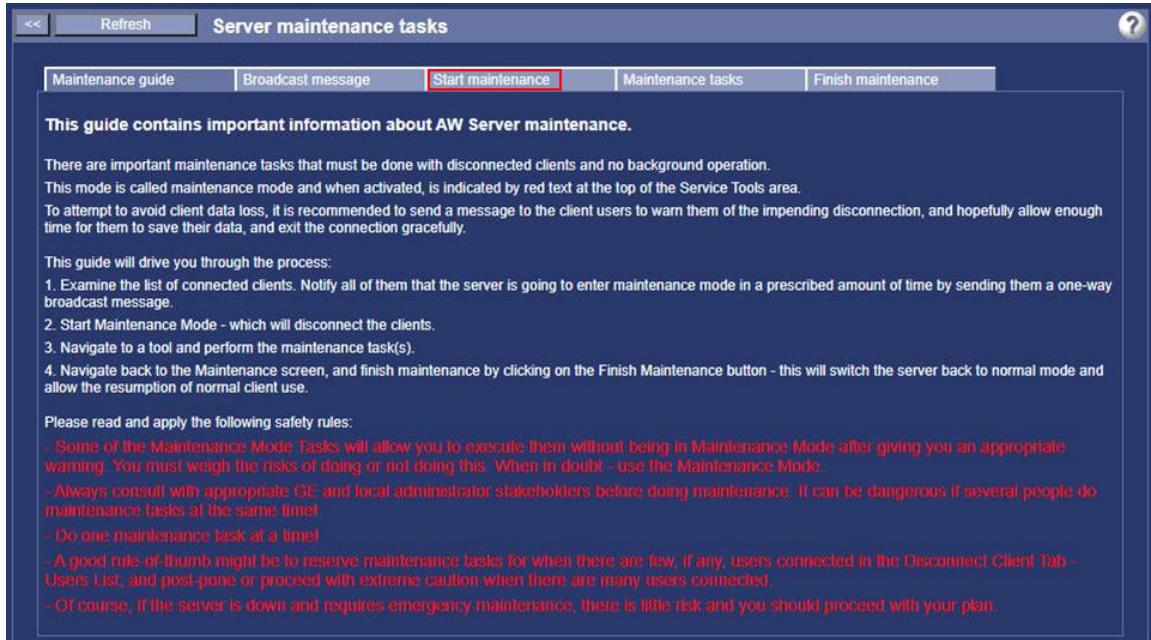
**NOTE**

If the AW Server is already in Maintenance Mode, skip this section.

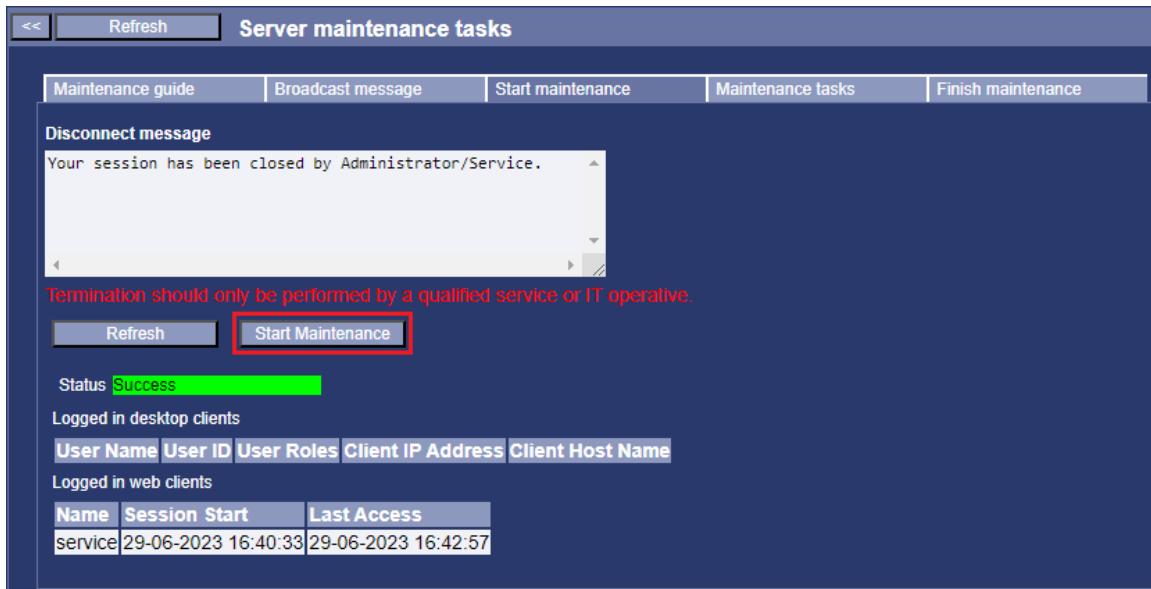
The Maintenance Mode allows the AW Server to be "isolated" from the AW Server Clients in order to perform maintenance operations such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters ...

Follow the below steps to place the AW Server in Maintenance Mode:

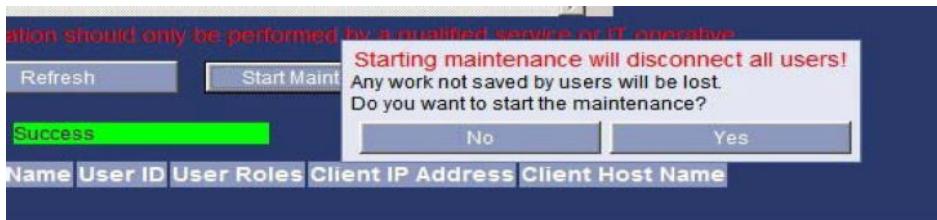
- From the Service Tools, select **Maintenance > Maintenance** and select the **Start maintenance** tab.



- Click on the **Start Maintenance** button to start the Maintenance Mode:



A pop-up confirmation message appears.



- Click on **Yes**.

Another pop-up states that you are in maintenance mode. And the Maintenance is in progress banner will display at the top of the Service Tools.

The screenshot shows the 'Service Tools - AW Server' interface. At the top, it says 'CST (3.2-3.2-975c1d6d) - AW Server ST (3.2-3.2-975c1d6d) [service]'. A red box highlights the message 'Maintenance is in progress since Jan 21, 2019, 6:14:11 PM'. Below that, it says 'Active Service Tools tasks: 0' and '• Global Installed Base data is not sent yet to GE!'. On the right, there's a 'Logout' link.

### 2.30.4.3 Backing up the configuration

- From the Service Tools, select **Maintenance > Backup > System configuration**.

The screenshot shows the 'Backup system configuration' screen. At the top left are 'Back' and 'Refresh' buttons. The main area has a heading 'Select as last known good configuration' with a checked checkbox. Below it is a note about network configuration not being part of the backup procedure. A list of items to select from includes Platform, Nuevo, Licensing, EA3, EAT, Smart card, ServiceTool, AW Server, RichClientUserPreferences, RSvP, AWS Service Tools, UPS Configuration, Mailcenter, IRIS, and ELS. To the right is a 'Comments' text area with a note about character set and two buttons: 'Pull from system' (highlighted with a red box) and 'Save on system'. At the bottom, there's a 'Recurrence' section with a start time of 16:41, an example of 14:46, and options for daily, weekly, or monthly recurrence. There are 'Activate' and 'Deactivate' buttons at the bottom.

- Check the **Select as last known good configuration** radio button.
- Keep everything selected and click on **Pull from system** to save the configuration in the /usr/g/ctuser/Downloads directory.

### 2.30.4.4 Loading the OS and AW Server Platform software Service Pack

- In case the Service Pack is delivered via RSvP:

If the NanoCloud AW Server is connected via RSvP and the Remove Software Download is supported, then 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.

The screenshot shows a red box highlighting the message 'Maintenance is in progress since Mar 25, 2021, 12:07:00 PM'. Below it, it says 'Active Service Tools tasks: 0'. A list of items includes:

- Global Installed Base data is not sent yet to GE!
- New package is available. **Click here for details** (highlighted with a red box)
- Remote Service (RSvP) is not properly configured or not running. **Click here for details**
- Last password generation and synchronization failed on Mar 28, 2021, 3:00:01 AM **Click here for details**

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 [2.30.4.5 Installing the OS and AW Server Platform software Service Pack on page 423](#).

2. In case the Service Pack has been copied to an USB media:

The AW Server Service Pack has been copied to an USB media in section [2.30.1.7 Copying the files prepared on the laptop into an USB media on page 380](#).

- a. In case you work remotely through FFA:

Insert the USB media into an USB port of the laptop and jump to [Step 3](#).

- b. In case you work locally at the CT Console, if the USB media is already mounted to /tmp/AWSUSB, jump to [Step 3](#).

#### **NOTE**

The USB media is automatically mounted to /tmp/AWSUSB if the Service Pack installation is part of an AW Server Installation/upgrade with the Installation Tool and the USB media is still plugged into the CT Console.

- c. Otherwise, mount the USB media manually:

- i. Insert the USB media into the CT Console.

- ii. In the Unix Shell (console/terminal) on the CT Console, login as **root**.

- iii. Mount the USB partition on the /mnt directory, by typing:

```
mount /dev/disk/by-label/AW_DATA /mnt <Enter>
```

3. From the Service Tools, select **Maintenance > Version Management**.

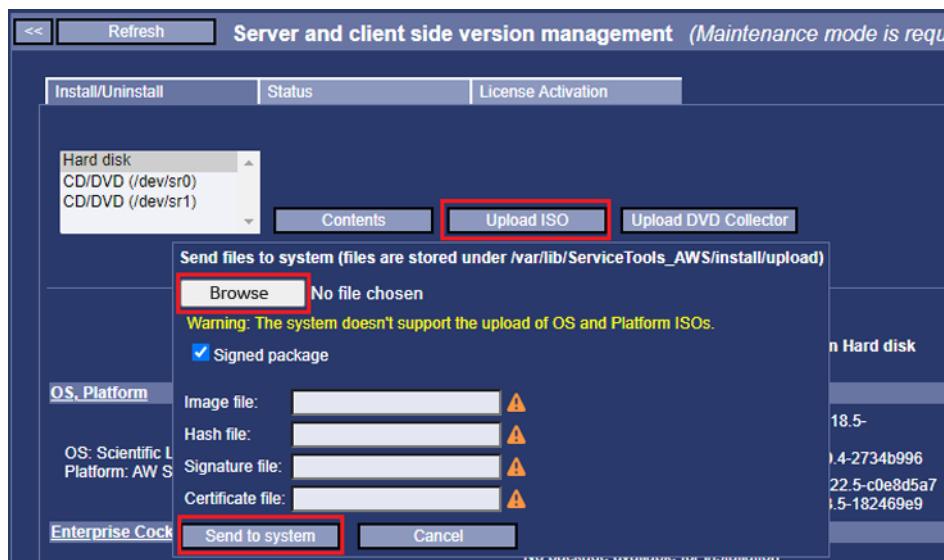
4. Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message.

5. Click on **Upload ISO** to upload the Service Pack.

#### **NOTE**

The Service Pack ISO file is a signed ISO. It 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.

6. In the pop-up window click on **Browse** and select the Service Pack ISO file as well as the hash, the signature and the certificate files, present on the USB media (search for .iso, .sha256.txt, .sha256.sig and .sha256.sig.pub extensions).



7. The **Image file** (Service Pack ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
8. To upload the ISO file click on **Send to system**.  
When the upload is completed, acknowledge the popup that displays.
9. Verify that the Service Pack appears in the Available for installation on Hard disk part of the page.
10. In case the USB media has been manually mounted in **Step 2.c**, unmount the USB partition and remove the USB media from the CT Console:  
`umount /mnt <Enter>`

## 2.30.4.5 Installing the OS and AW Server Platform software Service Pack

1. Select the AW Server Service Pack to install and click on **Install**.

The screenshot shows the 'Server and client side version management' interface. At the top, there are tabs for 'Install/Uninstall', 'Status', and 'License Activation'. Below these are buttons for 'Contents', 'Upload ISO', and 'Upload DVD Collector'. The main area is divided into two sections: 'Currently installed' and 'Available for installation on Hard disk'. Under 'Currently installed', there is a table for 'OS\_Platform' with entries for Scientific Linux release 7.9 (Nitrogen) and AW Server aws-3.2-4.9-2222.5-cbf960e7. Under 'Enterprise Cockpit and Web Applications', there is a table with no entries. Under 'Applications', there are two rows: one for 'Volume Viewer Apps 16.0-6.76' (with a red box around the 'Details' link) and another for 'AWServer 3.2 Ext. 4.9 Platform Service Pack 0.1' (which has a checked checkbox and a red box around both the 'Details' link and the package name). At the bottom, there are buttons for 'Uninstall', 'Install' (which is highlighted with a red box), 'Don't install', and 'Remove package'.

### 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.

2. 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. The actions recommended in this popup (except the reboot) will be done later.

3. Select the **Install/Uninstall** tab.
4. Check that the AW Server Service Pack appears in the **Currently installed** part of the page.

5. On the Healthpage, in **System Configuration** table, the **Modality OS Version** is updated.

Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9
Modality OS Version	AWS3.2_OS_7.2_SP_1.0 [20230109]
UDI	(01)00840682102384(10)AWS03D02E4D9SP1D0

6. Reboot the AW Server.

From the Service Tools, select **Tools > Reboot**, then select **Reboot AW Server**.

Wait for the AW Server to reboot, then login again into the Service Tools.

On the Healthpage, the **AWS Service Pack Version** displays in **Version Information**.

Version Information	
AWS Service Pack version	aws-sp-3.2.4.9-1.0

#### NOTE

If any issue occurs during the Service Pack installation or if the system does not work as expected after the Service Pack installation:

- Report the issue and contact an Online Service Engineer to collect the logfiles for further investigation.
- Use the backup created prior to install the Service Pack and reload the current AW Server (as for an upgrade – Load From Cold).

## 2.30.5 Applications Installation/Upgrade

#### Important

Follow this section only for the **installation or upgrade of Applications** on top of the **NanoCloud AW Server**. Otherwise, **skip** this section.

This section describes the steps to install/upgrade the applications on the AW Server.

The Applications are delivered either:

- In a Physical Software Kit.
- In a Digital Software Kit (eDelivery).

#### NOTE

For the systems connected via RSvP, if a new version of the Applications are available, they have been loaded onto the AW Server (from the software delivery portal).

#### NOTE

Repeat the below sections for any applications purchased by the customer (e.g.: Volume Viewer, SmartScore, ...).

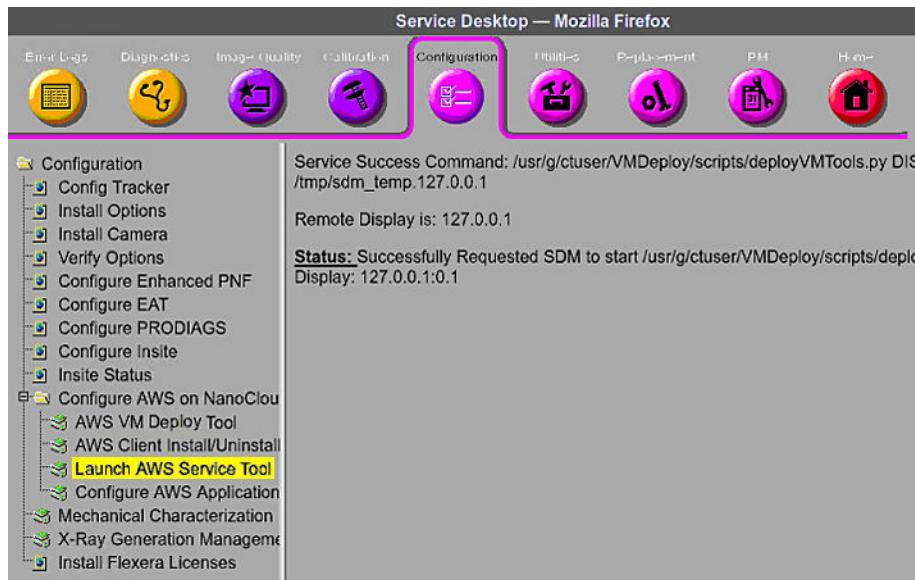
## 2.30.5.1 Launching Service Tools

#### NOTE

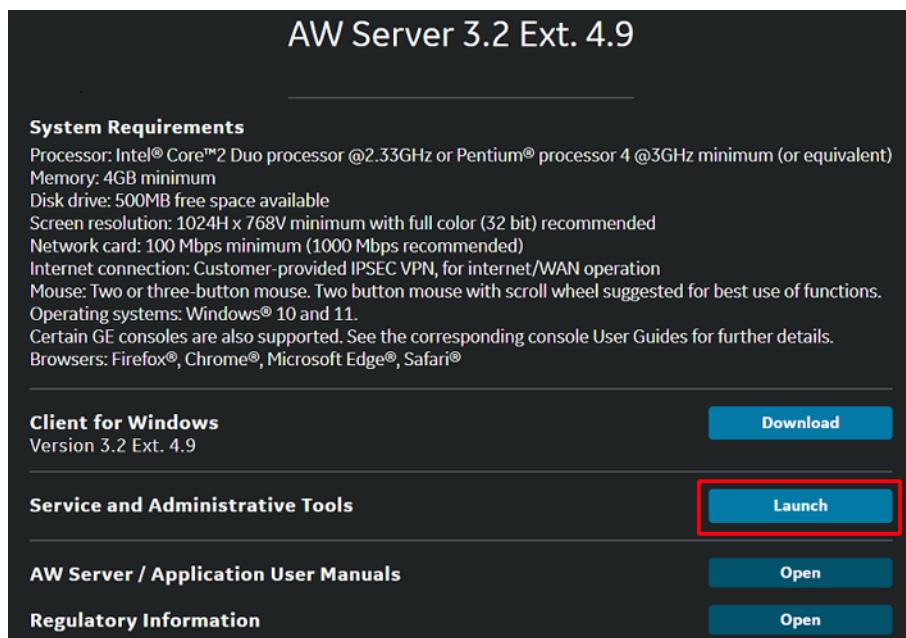
If the Service Tools is already launched, skip this section.

The Service Tools allows to configure the AW Server.

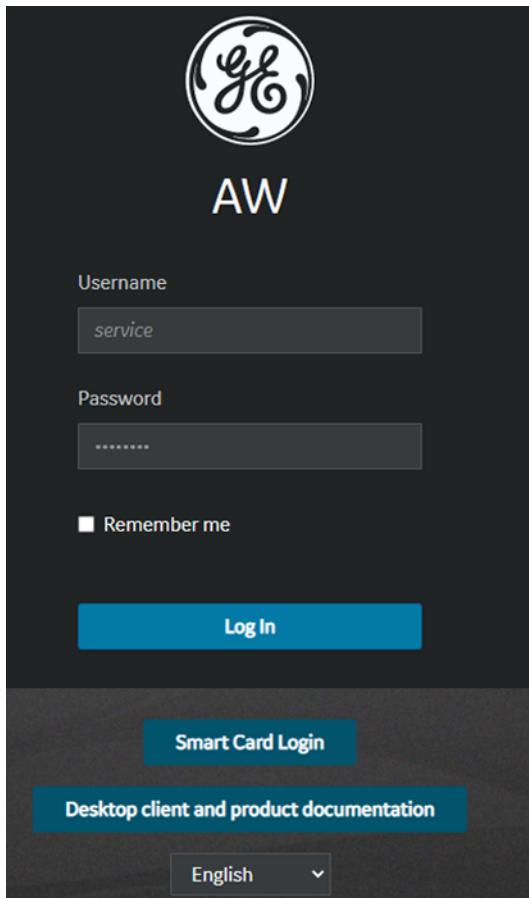
1. Start the Service Desktop interface using the CSD tool:



2. From the Service Desktop, select **Configuration > Configuration AWS on NanoCloud > Launch AWS Service Tools**.
3. Accept the cookies in the window that popups.
4. Click on the **Launch** button next to Service and Administrative Tools.



5. The login screen appears.



6. Login as **service**.

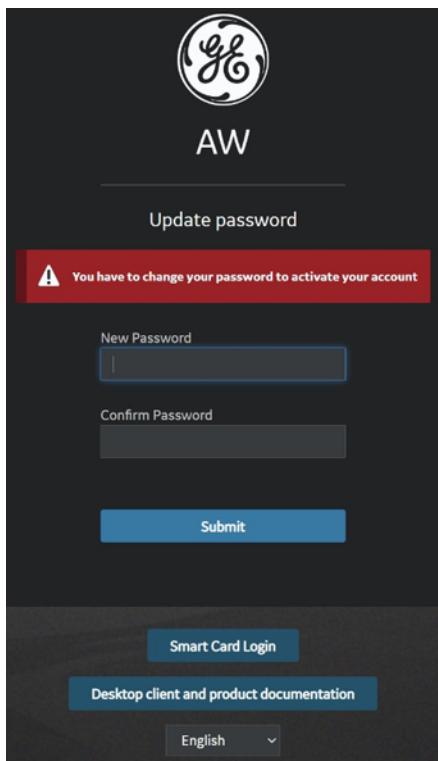
**NOTE**

If the password does not work, contact GE service and/or the site's IT admin to get the current password.

**NOTICE**

If the Internet browser proposes to remember the password for service account, and the FE is using a PC shared by other users, do not remember the password!

After successful login, if the password has expired (default passwords lifetime for local users is 60 days in RMF mode or 90 days in other modes, and for service/admin users is 1024 days) or the password needs to be changed at next login, the following screen displays:



Enter the new password, confirm it, and click on **Submit** button.

Refer to [2.30.6.2 Changing the Passwords on page 434](#) for the password change guidelines.

- The Service Tools opens with the installation/setup menus on the left.

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

System Configuration	
System ID (CRM Number)	BAY99_AWS
Platform version	aws-3.2-4.9-2241.4-b04b880e
Hostname / IP Address	bucaw70-239 / eth0: 3.249.70.239

#### NOTE

The **Close** link, next to the **Logout** link, allows to return to the main page (landing page) without logging out.

### 2.30.5.1.1 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, as shown below.

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.



#### NOTE

**Diagnostic** and **Tools** are not used for installation/setup.

**Administrative > Utilities** is not used for installation/setup.

### 2.30.5.2 Entering the Maintenance Mode

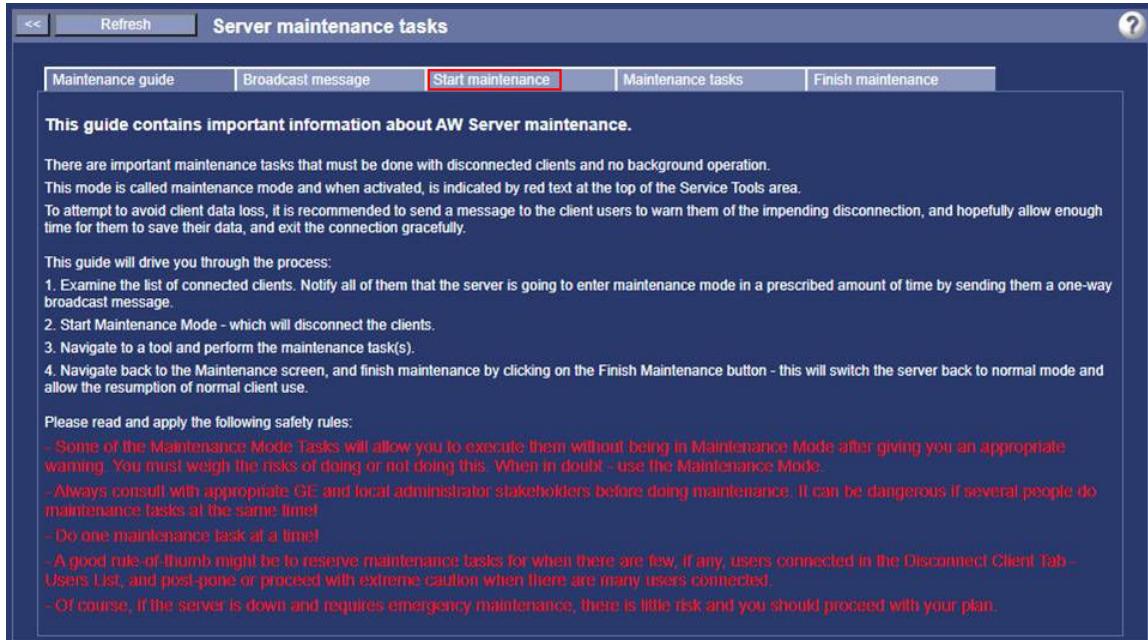
#### NOTE

If the AW Server is already in Maintenance Mode, skip this section.

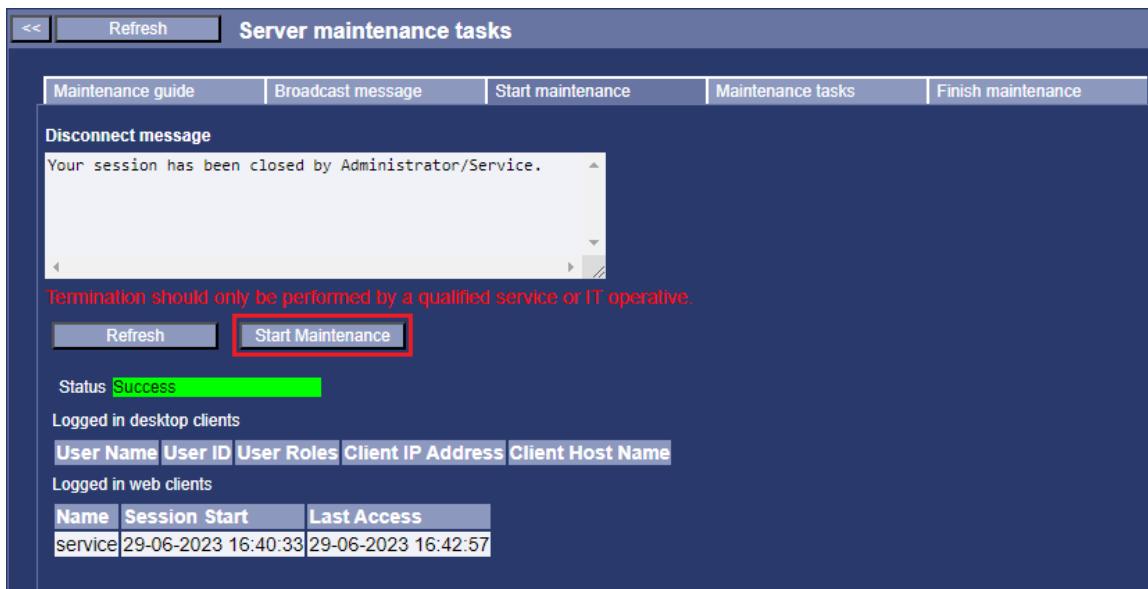
The Maintenance Mode allows the AW Server to be "isolated" from the AW Server Clients in order to perform maintenance operations such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters ...

Follow the below steps to place the AW Server in Maintenance Mode:

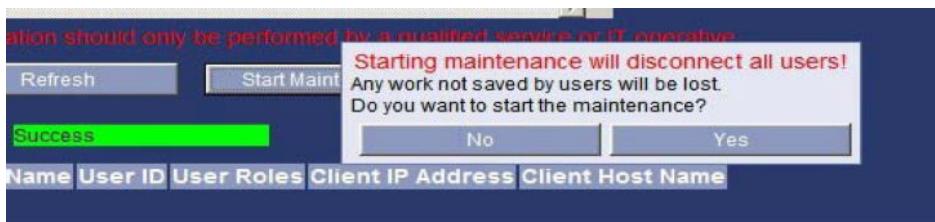
- From the Service Tools, select **Maintenance > Maintenance** and select the **Start maintenance** tab.



- Click on the **Start Maintenance** button to start the Maintenance Mode:



A pop-up confirmation message appears.



- Click on **Yes**.

Another pop-up states that you are in maintenance mode. And the Maintenance is in progress banner will display at the top of the Service Tools.



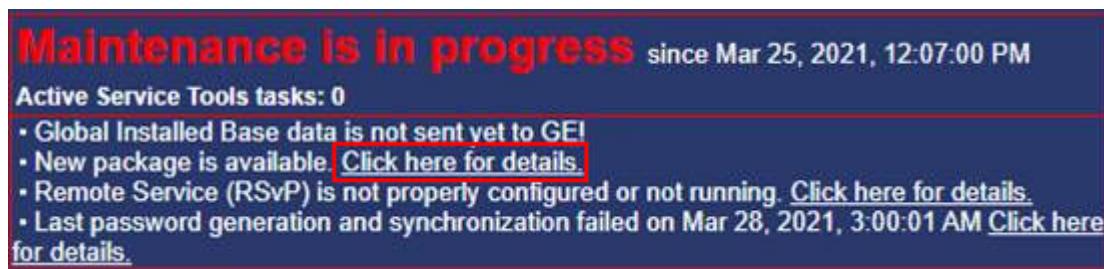
## 2.30.5.3 Loading the applications

This section describes how to load the applications (for a new installation) or to load new version of the applications.

1. In case the Applications are delivered via RSvP:

If the NanoCloud AW Server is connected via RSvP and the Remove Software Download is supported, then if new applications versions are available they have 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 install the applications in [2.30.5.4 Installing the applications on page 432](#).

2. In case the Applications have been copied to an USB media:

The Applications have been copied to an USB media in section [2.30.1.7 Copying the files prepared on the laptop into an USB media on page 380](#).

- a. In case you work remotely through FFA:

Insert the USB media into an USB port of the laptop, and jump to [Step 3](#).

- b. In case you work locally at the CT Console, if the USB media is already mounted to /tmp/AWSUSB, jump to [Step 3](#).

### NOTE

The USB media is automatically mounted to /tmp/AWSUSB if the Applications installation is part of an AW Server Installation/upgrade with the Installation Tool and the USB media is still plugged into the CT Console.

- c. Otherwise, mount the USB media manually:

- i. Insert the USB media into the CT Console.
- ii. In the Unix Shell (console/terminal) on the CT Console, login as **root**.
- iii. Mount the USB partition on the /mnt directory, by typing:

```
mount /dev/disk/by-label/AW_DATA /mnt <Enter>
```

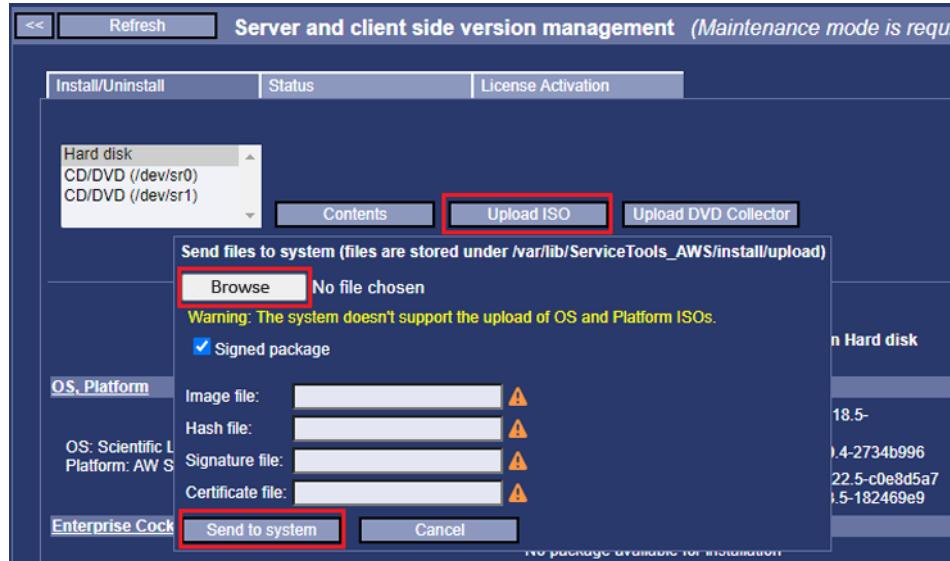
3. From the Service Tools, select **Maintenance > Version Management**.
4. Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message.
5. Click on **Upload ISO**.

- If the application ISO file is signed, follow the below substeps. Otherwise, jump to next step.

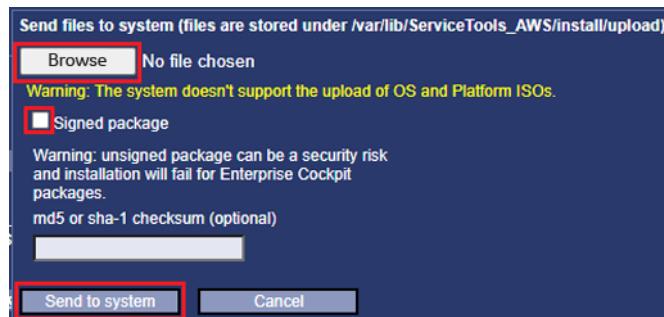
**NOTE**

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.

- In the pop-up window click on **Browse** and select the ISO file as well as the hash, the signature and the certificate files, present on the USB media (search for .iso, .sha256.txt, .sha256.sig and .sha256.sig.pub extensions).



- The **Image file** (component ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
- If the application ISO file is not signed, follow the below substeps.
    - In the pop-up window, uncheck the **Signed package** check box.
    - Click on **Browse** and select the ISO file present on the USB media.

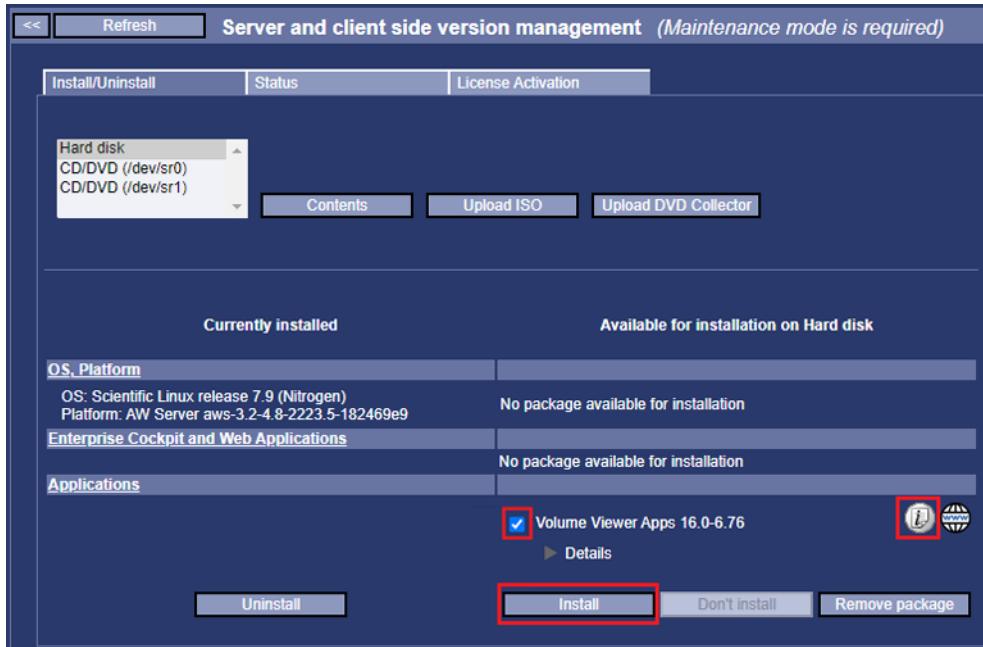


- For integrity check, copy/paste the md5 or sha-1 checksum of the ISO file, retrieved from the media, into the **md5 or sha-1 checksum (optional)** field.
- To upload the ISO file, click on **Send to system**.
- When the upload is completed, acknowledge the popup that displays.
- Verify that the application appears in the *Available for installation on Hard disk* part of the page.
  - In case the USB media has been manually mounted in [Step 2.c](#), unmount the USB partition and remove the USB media from the CT Console:

```
umount /mnt <Enter>
```

## 2.30.5.4 Installing the applications

- Select the application to install and click on **Install**.



### NOTE

For the systems connected via RSvP, if new applications versions are available, they have 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.

### NOTE

Application Software installation takes several minutes (~8 min for Volume Viewer).

When the installation is completed, acknowledge the popup that displays. The actions recommended in this popup will be done later.

- Select the **Install/Uninstall** tab.
- Check that the application appears in the *Currently installed* part of the page.

## 2.30.5.5 Activating the applications

- Select the **License Activation** tab.
- Click on **Select available** to automatically check the boxes of all licensed applications available on the Floating License Server.

3. Click on **Apply** to activate the application licenses.

Install/Uninstall		Status	License Activation	
Activated	Application Name	License Key String	License Information	Application Version
<input type="checkbox"/>	3D Suite	3D_Suite	PURENNH2TLX2RYHX	15.0-4.123
<input checked="" type="checkbox"/>	3D Viewer	Volume_Viewer	3Q5QGQC9NDLINESNF	15.0-4.123
<input type="checkbox"/>	Advantage CTC	CT_Colono_Pro3D_EC	CZXP0KSPY4LBMR	15.0-4.123
<input checked="" type="checkbox"/>	Autobone	AutoBone_Xpress	TZ0E57SXZJUP7NDF	15.0-4.123
<input type="checkbox"/>	Bone VCAR	Bone_VCAR	TEC4WAYBCK2ZF9H7	15.0-4.123
<input checked="" type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_MultiOrgan	DDZ3DPZ7HY6B98DM	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Myocardial	YSWQCVLWS86THH7C	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Neuro	ARYRTH69GRRDUOZ8	15.0-4.123
<input type="checkbox"/>	CT Perfusion 4D	CT_Perfusion_4D_Neuro_Enhanced	IVTKATDAD18TQVST	15.0-4.123

#### NOTE

If no change occurs (no new application have been installed), the **Apply** button remains greyed out and there is no need to reactivate the applications.

## 2.30.6 AW Server final Settings

This section describes the final settings prior to handover the AW Server to customer.

#### NOTE

This section requires to use the AW Server Service Tools. If they have been closed, refer to [2.30.2.3 Launching Service Tools on page 390](#) or [2.30.3.1 Launching Service Tools on page 399](#) to launch them.

#### NOTE

If only application(s) have been installed/upgraded, perform only sections [2.30.6.3 Registering the system configuration on page 441](#), [2.30.6.4 Backing up the configuration on page 443](#) and [2.30.6.5 Exiting maintenance mode on page 444](#).

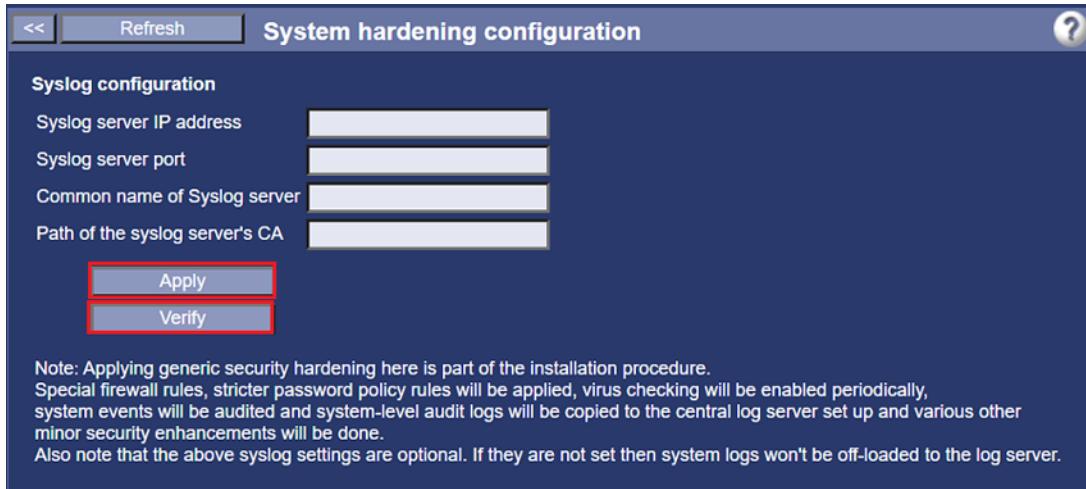
#### NOTE

To check the AW Server configuration or to manually configure the AW Server (for instance, in case the automatic configuration with the AW Server Installation Tool did not work during AW Server deployment) or for any additional settings on the AW Server, please refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#) and [2.18 Job Card IST010 - Administrative Configuration on page 184](#).

### 2.30.6.1 System Hardening

Improve the security of the system by enforcing the local user account password rules:

- From the Service Tools, select **Initial configuration > Hardening**.



- Leave the **Syslog configuration** fields empty and click on **Apply** button and then on **Verify** button.

**NOTE**

Once the *Running* indicator disappears next to the **Verify** button, the Hardening is ready.

## 2.30.6.2 Changing the Passwords

**Important**

Follow this section only for a **Load From Cold of the CT Software** or an upgrade of the **NanoCloud AW Server**. Otherwise, **skip** this section.

The account 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 passwords.

The default passwords are provided in the Advanced Service Manual, chapter 1 section 1.3.1 System Default Passwords.

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 requires that the server's system 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. **No system shall be handed over to the customer with the default root password under any circumstances**.

**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.**

**NOTICE**

When changing the passwords DO NOT MISS to notify the OLC representatives. Failing to do so would no longer allow access to your system from the OLC support teams.

### 2.30.6.2.1 Passwords Change Procedure

### 2.30.6.2.1.1 Identifying New Password(s)

The customer may request specific passwords. If this is the case, get the passwords from the customer and move on to [2.30.6.2.1.2 Changing Linux passwords- Optional on page 436](#). Make sure that the passwords chosen by the customer comply with the rules listed below.

#### NOTE

For the systems connected via RSvP, the passwords for **root** and **filetransfer** Linux users/accounts, are generated and synchronized with the RSvP server (GE Backoffice), as described in [2.30.6.2.1.2 Changing Linux passwords- Optional on page 436](#).

If a new password is to be created, the FE should do so in the following ways:

- If required, use customer rules and guidelines for password creation.
- If the FE is free to choose the password, use the following guidelines:
  - Must be 8 to 15 characters min. and 63 characters max.
    - 8 characters min. for AW Server user passwords (default value that can be changed)
    - 15 characters min. for Linux passwords
  - Must contain 1 digit
  - Must contain 1 upper-case letter
  - Must contain 1 lower-case letter
  - Must contain 1 non-alphanumeric character
  - Must not be a palindrome
  - Must not be blank or left as the default
  - Must not be made up solely of dictionary words or easily guess
  - Must not contain 3 consecutive identical characters
  - Must not contain a blank space
  - Must not include your logon name
  - Should not be the same value at different sites

Good password examples:	Bad password examples:
<b>!414585MR5test\$</b>	<b>414555AWS5</b>
<b>4\$42CTAWSERVER32</b>	<b>operator</b>
<b>big996622LS16ct*</b>	<b>123456789a</b>

The following characters (which the system may assign a special meaning) should be avoided:

**@ ; # ; <Tab> ; <Esc>** ; etc .... However, **#** can be used for the **root** password.

#### NOTICE

Each account on a single system should have a unique password. For example, the **root** and **service** accounts should have different password values from each other. Using the same password for multiple accounts on a system will remove role-based access and decrease the level of security on a system.

For productivity, the same password value for a single account can be used on multiple systems at a site or customer. For example, the **root** user/account could have the same non-default password value on 3 different systems in a hospital. However, make sure not to use the same value over multiple sites or across a region, because that would essentially duplicate the original default

value problem this service note attempts to resolve. For this reason, procedures are given below for alternative AW platform releases.

### 2.30.6.2.1.2 Changing Linux passwords- Optional

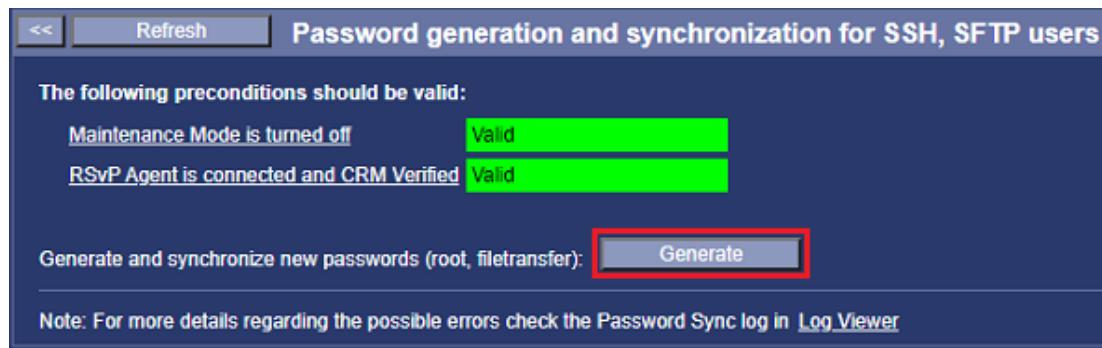
To change the passwords for **root** / **filetransfer** Linux users/accounts follow the below steps:

1. If the system is connected via RSvP, the passwords for **root** and **filetransfer** Linux users/accounts, can be generated and synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault:

**NOTE**

In case of a full AW Server installation the Linux passwords can be changed later as the Configuration must be registered prior to turn off the Maintenance Mode

- a. From the Service Tools, select **Administrative > Configuration > Users (OS)**.



- b. The Maintenance Mode must be turned off. If the status is **Invalid**, click on **Maintenance Mode is turned off** to open the *Server maintenance tasks* page. In this page, select **Finish maintenance**.
- c. The RSvP Agent must be connected and CRM Verified. If the status is **Invalid**, click on **RSvP Agent is connected and CRM Verified** to open the RSvP configuration page. Refer to [2.30.2.4.1 Setting up Remote Service on page 394](#).
- d. Click on the **Generate** button to generate the new passwords for **root** and **filetransfer** Linux users/accounts and synchronize them with the RSvP server (GE Backoffice).
- e. Remotely through FFA, display the *System Password Vault* panel.

The screenshot shows a table titled "System Password Vault" with the subtitle "The vault is only password storage for RSvP devices. Changes here will not affect the actual device.". The table has columns: #, App Name, Username, Password, Last Updated, Updated By, and Actions. There are three rows: 1. App Name: ea3, Username: service, Password: [REDACTED], Last Updated: Feb-17-2021 12:02:58, Updated By: AGENT, Actions: Show, Copy, Change Password. 2. App Name: sftp, Username: filetransfer, Password: [REDACTED], Last Updated: Feb-18-2021 12:10:59, Updated By: AGENT, Actions: Show, Copy, Change Password. 3. App Name: ssh, Username: root, Password: Uz\$Un3f+ONaznezA SiM.UwwiMKi, Last Updated: Feb-18-2021 12:11:10, Updated By: AGENT, Actions: Hide, Copy, Change Password. The "root" password is highlighted with a red box.

- f. Select the **Show** link to view the new password.

**NOTE**

New passwords are generated and synchronized on a weekly basis, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified.

2. If the system is not connected via RSvP, the Linux passwords for **root** can be changed using a command line window:
  - a. Open a command window:
    - via the **virt-manager** to display the AW Server Console
    - or via the **SSH** connectivity tool or the **Terminal** tool in FFA.
  - b. Login as **root**, using the current **root** password.
  - c. To change the current password, type:  
**passwd <Enter>**
  - d. Type the new password and press **<Enter>**.
  - e. To confirm the new password, type it again and press **<Enter>**.
  - f. Logout and login again to apply the change.
3. It is STRONGLY RECOMMENDED to test the new passwords before turnover to customer, in order to make sure that there was no typo or mix-up with the local keyboard when the password was changed.
  - a. Open another command-line window.
  - b. Login with each Linux users/accounts and enter the new passwords.

The operating system is configured to lock accounts for a minimum of 15 minutes after five unsuccessful logon attempts within a 15-minute timeframe. The operating system is configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds. Do not use the **authconfig** tool in the operating system for authentication configuration, it may overwrite the system hardening settings.

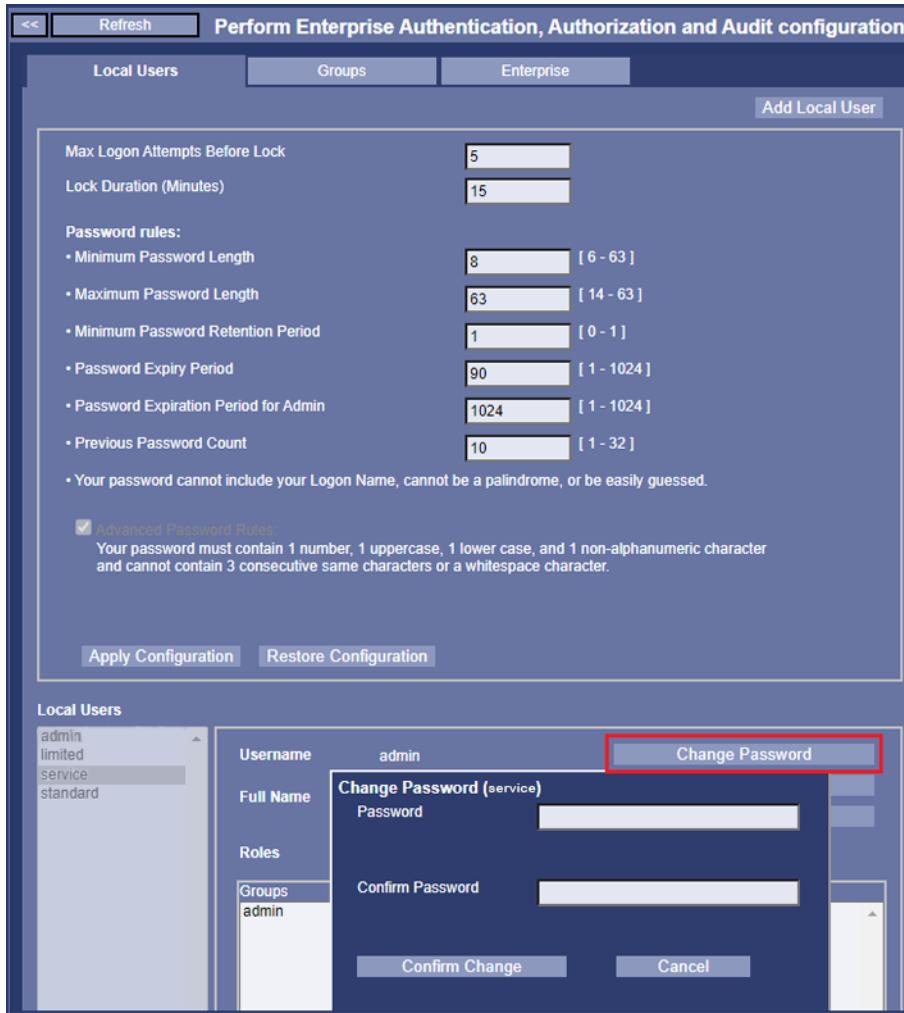
**NOTE**

This fail lock mechanism does not apply to the **root** Linux user account.

### 2.30.6.2.1.3 Changing the service Password

The default **service** password is provided in the Advances Service Manual, chapter 1 section 1.3.1 System Default Passwords.

- From the Service Tools, select **Administrative > Configuration > Users (EA3)**.



- In the **Local Users** area, select **service** account and click on the **Change Password** button.
- In the **Change Password** window enter the new password and confirm it.

#### **NOTE**

The default password rules can also be changed in this page.

- To confirm the new password, click on **Confirm Change**.
- Click on **Apply Configuration** button.
- Synchronizing the service password with RSvP:

If the system is connected via RSvP, the **service** password is synchronized with the RSvP server (GE Backoffice) and can be viewed using the FFA System Password Vault, provided that the Maintenance Mode is turned off and the RSvP Agent is connected and CRM Verified:

- a. 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	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
2	sftp	filetransfer	*****	Jun-14-2021 19:07:31	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>
3	ssh	root	*****	Jun-14-2021 19:07:34	AGENT	<a href="#">Show</a> <a href="#">Copy</a> <a href="#">Change Password</a>

- b. Select the **Show** link to view the new password.

### 2.30.6.2.2 Updating Password(s) in Connectivity Database

Update the password in the Connectivity Database and notify the OLC representatives, as described in the table below.

Region	Connectivity Center Information
AMERICAS (US, Canada)	USCAN Connectivity Support toll-free number: 877-842-1132 (8am – 6pm CST, Mon-Fri)
LatAm	Preferably reach the connectivity team via <a href="https://sc.ge.com/*LATAMcheckout">https://sc.ge.com/*LATAMcheckout</a>  or call +55 11 8000 164 702
EU and EMEA	Use the Support Central EMEA Password Change workflow <a href="https://sc.ge.com/*emeapwc">https://sc.ge.com/*emeapwc</a> 
Japan	Call the Connectivity Support number: 0120 596 919
ASEAN	Contact OLE or connectivity champion for re-checkout the system.
ANZ	Call the Connectivity Support numbers Australia 1800 659 465 or New Zealand 0800 659 465 OR open a case at <a href="http://sc.ge.com/*ANZConnectivity-Support">http://sc.ge.com/*ANZConnectivity-Support</a>
Korea	Call the Connectivity Support (OLC support) number : 1544 6119

China	Call the Connectivity Support number : 400 812 8188 OR contact OLE for system checkout/re-checkout
India	Call the Connectivity Support number : 1800 102 7750 (India Call Center) ext 4

### 2.30.6.2.3 Communicating New Password(s)

1. Follow your customer's guidelines for password communication and storage. Inform the customer of the new passwords with the exception of those used for remote service only.
2. If the customer approves, write down the new passwords and store them in a secure location on site.  
The [2.30.6.2.4 Password Form on page 440](#) includes a sample form to place in a logbook or tape inside a cabinet.
3. In the situation where a customer wants to know more about what GE does with passwords, escalate to the service security team at:  
[http://supportcentral.ge.com/products/sup\\_products.asp?prod\\_id=295163](http://supportcentral.ge.com/products/sup_products.asp?prod_id=295163)

### 2.30.6.2.4 Password Form

 GE Healthcare

Password Change Record for  
System ID \_\_\_\_\_  
By \_\_\_\_\_  
Date \_\_\_\_\_

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Login ID	
Password	

Copyright Pending

The passwords configuration is complete.

### 2.30.6.3 Registering the system configuration

- From the Service Tools, select **Maintenance > Register Configuration**.

**Status**

licenseld:  
068abc98

**Registration Key status:**  
Registration Key : BSADDRNRJYFMNAGB  
Registration Status : Invalid

**Connectivity Status :**  
Configuration Registration(AWCCT) Server not reachable

**Install Registration Key**

Registration Key :

If you have a valid Registration Key, enter it in the field above to complete registration

**Auto Register**

If the system is connected to GE (InSite), click this button to export configuration to AWCCT. If configuration is valid, a Registration Key is returned and automatically installed on the workstation.

**Export Configuration (Manual Registration)**

**Instructions :**

If the system is not connected to GE, and valid Registration Key not available:

- Click button above to export the configuration file to Hard disk
- Upload this file to <https://awcct.gehealthcare.com> to get a Registration Key. If you cannot connect from the system, try from a PC with internet access.
- Install the Registration Key on the system to enable software/applications

- Automatic Registration:

If the AW Server is connected via RSvP and that the System ID (CRM Number) is verified, you can use the Automatic Registration process.

- Click on the **Perform Auto Registration** button, to automatically send the Site configuration file to the AWCCT Web site.

If the configuration is compliant, messages will say so in the **Connectivity Status** and **Registration Status** areas on the left of the page and you will automatically receive in return within a few seconds the Registration key, while at the bottom left of the page, the message Request in progress appears, followed by Operation success.

- The **Registration status** field in the HealthPage should display as Standard in green.

Bypass the next steps. They are dedicated to manual registration when remote connection via RSvP is not available.

- Manual Registration:

If the AW Server is NOT connected via RSvP, perform a manual registration.

- Click on **Export Configuration** to export the configuration file and save it on the CT Console in /usr/g/ctuser/Downloads.
- Copy the system configuration file into an USB media:
  - Insert the USB media into the CT Console.
  - If not already done, open an Unix Shell (console/terminal) on the CT Console.

- iii. Mount the USB media:

```
mountUSB <Enter>
```

- iv. Navigate to the /usr/g/ctuser/Downloads directory and list its content in chronological order:

```
cd /usr/g/ctuser/Downloads <Enter>
```

```
ls -altr <Enter>
```

**NOTE**

The files are listed in chronological order. Meaning that if more than one file are listed, the system configuration file is the latest file displayed.

- v. Copy the system configuration file in to the USB media:

```
cp <LicenseID>_<SystemID>_<DateTime>_Configuration.txt /USB <Enter>
```

- vi. Unmount the USB media.

```
umountUSB <Enter>
```

- c. In an Internet Navigator connect to <https://awcct.gehealthcare.com> and upload the configuration file:

Submit Advantage Workstation Configuration File(AW/AW Server/AW Pioneer)					
Select configuration file to Upload : *	<b>Choose File</b>	068abc98_...nfiguration.txt			
Any Comments/Suggestions :					
<b>Submit</b>	<b>Reset</b>				

- Click on **Choose File**, then select the configuration file previously exported.
- Click on **Submit** to generate the registration key.

File Name	File Upload Status	Registration Key	System ID	License ID	View Details
068abc98_AWBULAB240_100005286_AWS_20201230160121.txt	Success	FNKLOZJIBXDJHJ	AWBULAB240	068abc98	<a href="#">Click here</a>

- d. Type in the registration key into the **Registration Key** field and click on **Install Registration Key**.

**Install Registration Key**

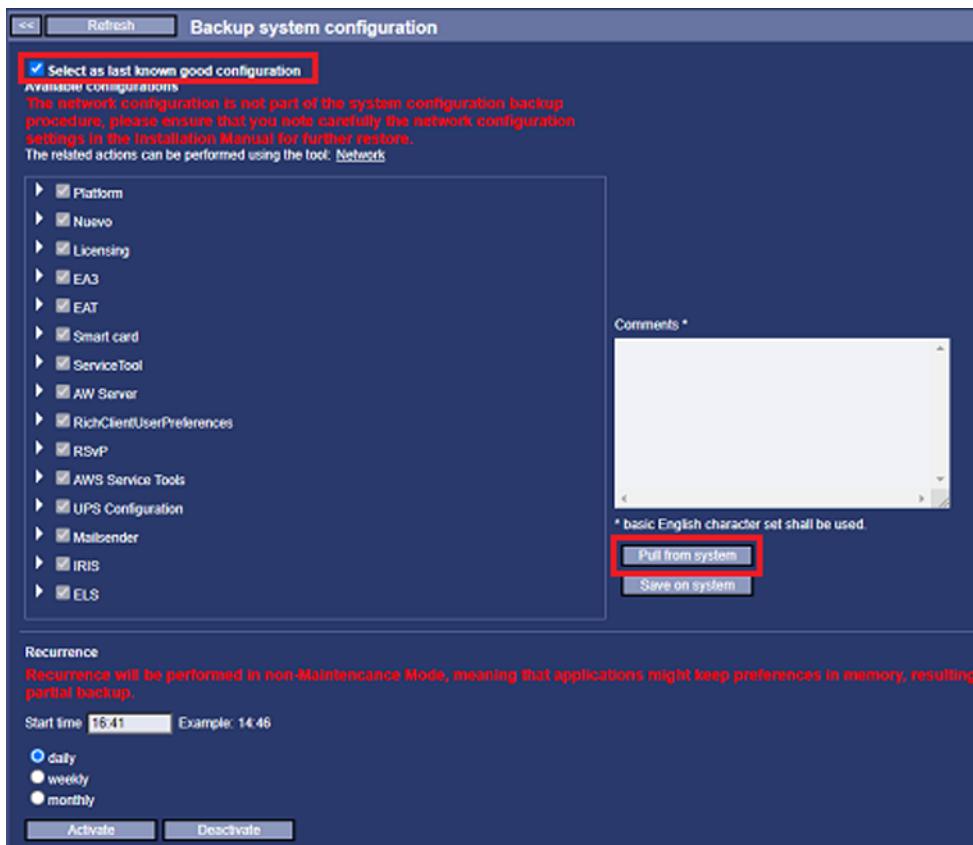
Registration Key :  **Install Registration Key**

If you have a valid Registration Key, enter it in the field above to complete registration

At the bottom left of the page, the message Request in progress appears, followed by Operation success.

## 2.30.6.4 Backing up the configuration

- From the Service Tools, select **Maintenance > Backup > System configuration**.



- Check the **Select as last known good configuration** radio button.
- Keep everything selected and click on **Pull from system** to save the configuration in the `/usr/g/ctuser/Downloads` directory.
- Copy the saved configuration on an USB media and keep it in a safe place:
  - Insert the USB media into the CT Console.
  - If not already done, open an Unix Shell (console/terminal) on the CT Console.
  - Mount the USB media:

`mountUSB <Enter>`

- Navigate to the `/usr/g/ctuser/Downloads` directory and list its content in chronological order:

`cd /usr/g/ctuser/Downloads <Enter>`

`ls -altr <Enter>`

### NOTE

The files are listed in chronological order. Meaning that if more than one file are listed, the configuration backup file is the latest file displayed.

- Copy the configuration backup file in to the USB media:

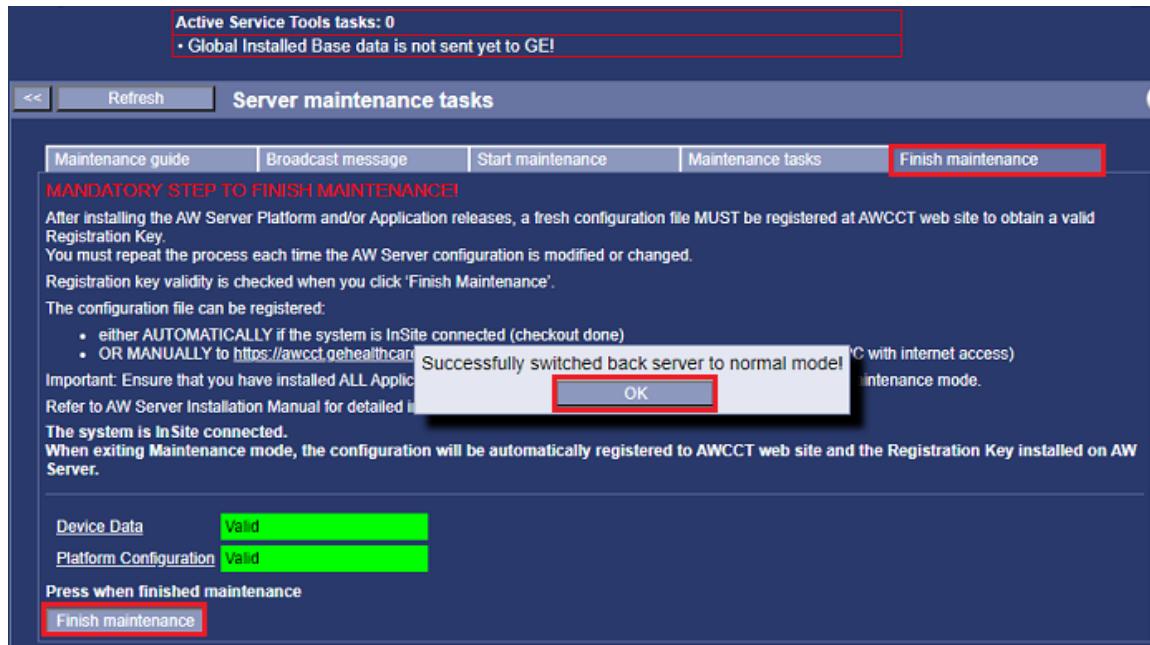
`cp <SystemID>_backupSyst_<Date_Time>.tar.gz /USB <Enter>`

- Unmount the USB media:

`umountUSB <Enter>`

## 2.30.6.5 Exiting maintenance mode

- From the Service Tools, select **Maintenance > Maintenance > Finish maintenance**.
- Click on **Finish maintenance**.
- In the pop-up window, click **OK**.

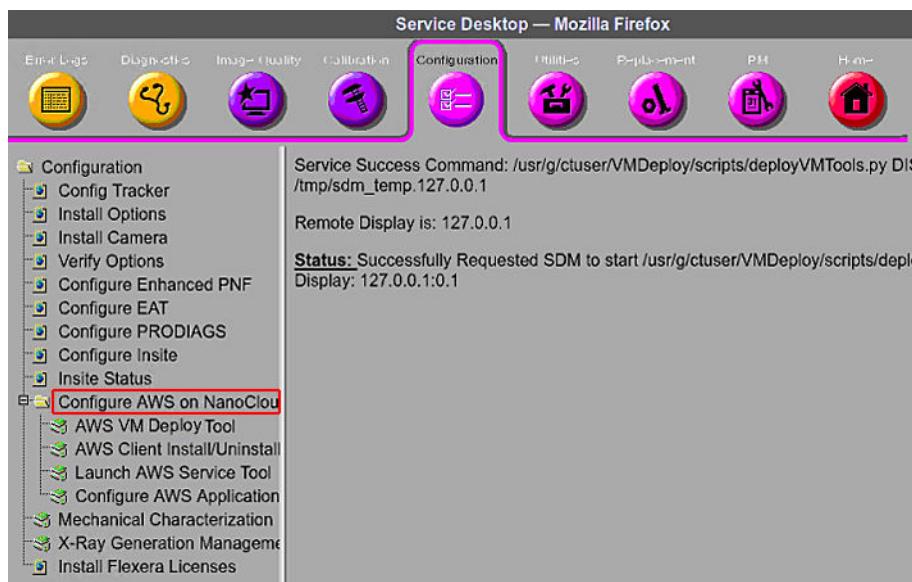


- If not already done, remove the USB media from the CT Console.

## 2.30.7 Installing AW Server Client on CT Console

This section describes the AW Server Client installation/update and configuration in the CT Console, and check the AW Server Client connectivity.

- Start the Service Desktop interface using the CSD tool and select **Configuration > Configuration AWS on NanoCloud**.

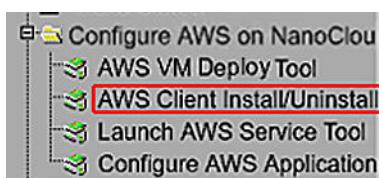


**NOTE**

If you do not have the Insite/RSvP connectivity, you should establish a **ssh** connection to the CT Console with X11 tunnel. This can be done with **PuTTY** (or equivalent tool) by enabling **SSH X11 forwarding** option. Then you can login with **ssh** to the CT Console and type in the terminal: **firefox <virtual private subnet>.5**.

For instance: **firefox 192.168.101.5**

2. From the Service Desktop, select **AWS Client Install/Uninstall**.

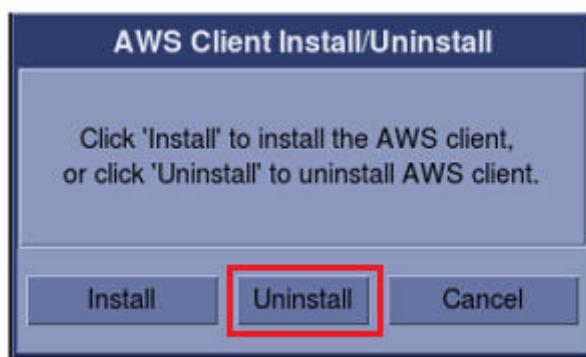


3. Install the AW Server Client:

**NOTE**

In case of an **upgrade** of the **NanoCloud AW Server** and in case of an **upgrade** of **Applications** or **installation** of **patches** on top of the **NanoCloud AW Server**, the AW Server Client should be uninstalled prior to reinstall it:

- a. Select **Uninstall** in the popup that displays.



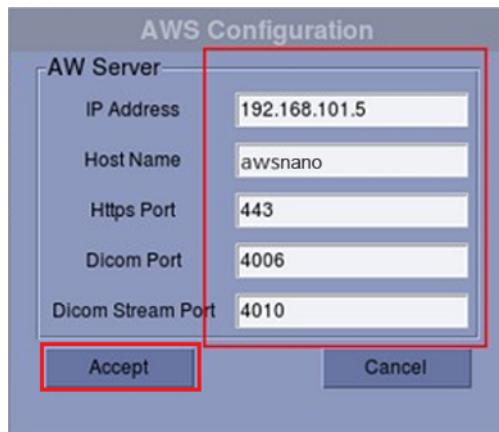
The uninstallation is completed once the popup disappears.

- b. Click again on **AWS Client Install/Uninstall**.

Select **Install** in the popup that displays.



4. Check the information in the window that displays. Then click on **Accept**.



**NOTE**

Update the **IP Address** to 192.168.102.5 if the virtual private subnet used during installation was 192.168.102.x.

5. From the Service Desktop, select **Configure AWS Applications**.

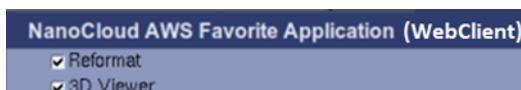


6. The **Favorite Application** window appears. The headline of this window defines the AW Server Client type:

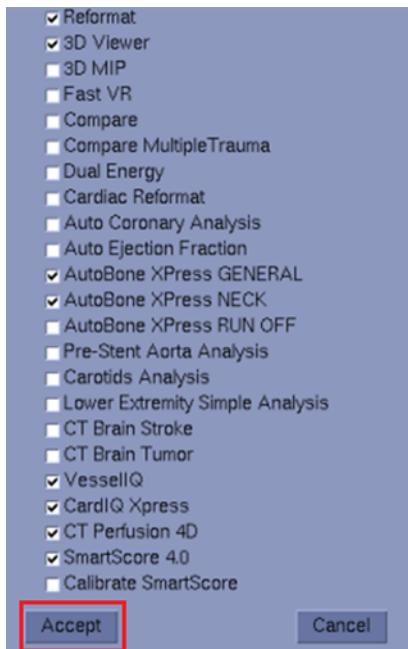
- The headline is **NanoCloud AWS Favorite Application** for a standard AW Server Client:



- The headline is **NanoCloud AWS Favorite Application (WebClient)** for the AW Server Web Access:



7. In the **Favorite Application** window, select your applications then click on **Accept**.



**NOTE**

Refer to the project manager to select the applications available for your site.

**NOTE**

If the **AW Server Certificate** window pops up, accept the certificate.

8. Reboot the CT Console.

**NOTE**

After the restart of the CT Console, the AW Server is usually available 5 to 10 minutes later. This is only an estimated time, and the actual delay will vary depending on the hardware host and CT Console configuration.

9. Check AW Server Client connectivity:

- a. Switch to the **ImageWorks** desktop.
- b. In the Browser, select a scan instance.
- c. Select an application prefixed by **AWS** (for instance **AWS Reformat**). The application starts.

**NOTE**

Acknowledge the popup window related to certificate if any.



## 2.31 Secured for RMF mode

### 2.31.1 RMF hardening package

RMF stands for Risk Management Framework (in cybersecurity context). It is a collection of processes and policies addressing security of information systems. AW Server supports Secured for RMF mode. In this mode, several STIGs (Security Technical Implementation Guide) are applied satisfying RMF requirements. During the software installation of the AW Server, a package containing all the tools needed to enable this mode is installed on system. If Secured for RMF mode needs to be turned on, it requires an extra step after the software installation. Start the hardening process using the preinstalled package.

### 2.31.2 AW Server Configuration and Limitations in Secured for RMF mode

In this mode:

- The AW Server can only work in Standalone (No-integration) mode.  
Only the following type of installation procedures are supported:
  - Fresh installation.
  - Reinstallation of an AW Server already in Secured for RMF mode.
  - Re-activating Secured for RMF mode after Application or Service Pack installation or after restore from backup.
- DICOM hosts: DICOM communication can only be configured using TLS (TCP port **2762** by default - the TCP port **4006** used for plain (unsecure) DICOM communication is not allowed and that port is disabled in firewall). Refer to [2.18.1 Configuring DICOM hosts in Service Tools on page 184](#).

#### NOTE

FE can configure exceptions for DICOM sources which do not support TLS after the Secured for RMF activation. See details in [2.31.3.4 Interoperability with non-RMF compliant systems on page 462](#).

- The following functionalities are disabled or shall not be configured/used in the AW Server:
  - Media Creator.

- Free Image Importer.
- DICOM printing.
- Postscript printing.
- Remote Connectivity (RSvP, IRIS, Prodiag, Sweep etc.).
- External CoLA license server access.
- Screen Sharing.
- SNMP configuration.
- File transfer and upload features.
- Imaging Cockpit / Web client.
- System hardening configuration.
- Event Synchronization between Universal Viewer and 3D Applications (dotMed service disabled).
- Features provided by Result Management Platform (RMP) service.
  - Copying images from AW Server client to clipboard.
  - Sharing application report documents on the client.
- The following functionalities are partially disabled in the AW Server:
  - Only Volume Viewer applications are supported in RMF mode.
  - **Service Tools > Maintenance > Version Management** page accepts only signed iso packages.
  - Only built-in CoLA server configuration is available. Remote CoLA server access is disabled.
  - Time Settings shall be configured to connect AW Server to the Hospital's central Time Server (NTP server). See details in [2.15.6 Time Settings on page 148](#).

#### NOTE

The connection to the Time Server must be secure, which require NTP symmetric key scheme authentication. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 9](#).

- AW Server must send audit and certain log messages to Hospital's central log servers (Syslog server and audit log server).

#### NOTE

AW Server in RMF mode sends different log and audit messages to Hospital's central log server (Syslog server) and the Hospital's central audit log server (auditd):

- OS-level System logs (rsyslog) and Application-level audit logs (EAT) are sent to the Syslog server.
- OS-level auditd messages (through audisp-remote) are sent to the audit log server.

To achieve full RMF compliancy, AW Server must secure the channel used for sending auditd messages. Therefore AW Server uses Kerberos authentication to send the auditd messages to the Hospital's central audit log server (auditd) in a secured channel. It is switched on during RMF activation. It can be decided not to use secured channel by answering **No** to the related question during RMF activation, but this will result in only partial RMF compliance. See [2.31.3.2 Executing the Hardening process on page 456](#).

**NOTE**

It is the Customer's responsibility to prepare the Hospital's environment for the Kerberos authentication. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 2](#).

- MailSender is not disabled. It displays security warnings to warn the user to use this feature with care.
- Backup/Restore:
  - Systems where the secured mode was not selected yet (only fresh installation scenario):
    - Backups created in "Secured for RMF" mode are accepted. But, this system should operate only in "Secured for RMF" mode afterwards.
  - Systems with "Secured for RMF" active only accept backups created in "Secured for RMF" systems.
  - Non-RMF systems where System Hardening was already activated, cannot accept backups created in "Secured for RMF" systems.

**NOTE**

According to DoD policies backup shall be done at regular intervals and these backups should be stored offsite with appropriate physical and technical protection.

- GIB data transfer: Send via PC disabled.
- Register Configuration: Register configuration and generate configuration file shall be performed using command line solution instead of using the Register Configuration UI. See details in [2.31.3.5 Configuration registration solution in RMF \(DoD\) mode on page 465](#).
- External server connections must be secured with TLS and TLS1.2 protocol will be enforced.

**NOTE**

FE can configure exceptions for DICOM sources which do not support TLS after the Secured for RMF activation. See details in [2.31.3.4 Interoperability with non-RMF compliant systems on page 462](#).

- AW Server certificate shall be signed with external, DoD approved Certificate Authority (CA) selected by the Customer.

**NOTE**

Be aware that certificate signing with an external CA might take significant time. It can vary from 1-2 hours up to several days. Discuss the schedule with the Customer in advance.

- RMF activation does not accept self-signed AW Server certificate. AW Server certificate must be signed with an external, DoD approved Certificate Authority (CA) selected by the Customer.

**NOTE**

GE responsibility is to provide the Certificate Signing Request (CSR), the actual signing is the responsibility of the Customer.

- USB connection and SSH access are disabled.

In Secured for RMF mode AW Server will enable SSH and USB for the Maintenance period.

- User Management: Enterprise Authentication is mandatory to achieve full RMF compliancy.

Local user management service (EA3) of AW Server does not have full RMF compliancy, therefore configuring Enterprise Authentication is mandatory. Refer to [2.18.4.2 Configuring Enterprise User\(s\) Accounts on page 195](#).

- The following functionalities are replaced in the AW Server:
  - ClamAV will be replaced with McAfee Antivirus software.
  - Secured for RMF mode enforces more strict password policy rules.

## 2.31.3 Activating the Secured for RMF mode

### NOTE

Once Secured for RMF mode is activated and the system has been hardened there is no way to revert back from DoD mode into generic mode except a full system reinstallation.

Before activating the Secured for RMF mode (starting the hardening process) on the AW Server, do the following steps:

1. For Virtual AW Server, ensure that the disk encryption is set on the customer hardware supporting the Hypervisor environment hosting the Virtual AW Server. Since the hardware supporting the Hypervisor environment for Virtual AW Server is under the Customer's responsibility, the disk encryption is also the customer's responsibility.
2. Install and configure the AW Server.

Perform the installation as in the case of a "normal" (Generic mode) AW Server and do all steps till getting to registering configuration and exiting Maintenance mode.

### NOTE

Stop with the procedure there. **Do not perform** System Hardening, **do not perform** Configuration registration, **do not exit** Maintenance mode and **do not perform** Server validation tests at this stage. These steps (except System Hardening) shall be performed **only after successful RMF activation** and will be described in this chapter later.

The specific sections in this document will describe what steps to perform in specific way and/or what not to do in case of Secured for RMF mode activation.

3. Optional: In case of a reinstallation of an RMF system, restore the Last known good backup created on the system when Secured for RMF mode was activated.
4. If not done yet, configure the connection to the Hospital's DNS server, so AW Server can resolve the host names and URLs of the connected servers.
  - Refer to [2.13 Job Card IST005 - Network and Time Configuration on page 127](#).
  - In case you want to configure it after the initial installation refer to [A.8.8 DNS server\(s\) setup - Alternate method on page 594](#).
5. If not done yet, perform AW Server certificate signing with external, DoD approved Certificate Authority (CA) selected by the Customer (RMF activation does not accept self-signed AW Server certificate). See details in [2.18.11.5 Renewing the AW Server certificate on page 215](#) and [2.18.11.5.2 Renewing AW Server external CA signed certificate on page 217](#).

### NOTE

Be aware that certificate signing with an external CA might take significant time. It can vary from 1-2 hours up to several days. Discuss the schedule with the Customer in advance.

6. If not done yet, configure Enterprise Authentication in **Service Tools > Administrative > Configuration > Users (EA3)**.

Local user management service (EA3) of AW Server does not have full RMF compliancy, therefore configuring Enterprise Authentication is mandatory. Refer to [2.18.4.2 Configuring Enterprise User\(s\) Accounts on page 195](#).

To achieve full RMF compliancy switch on "Use SSL" and "Verify Certificate" during the Enterprise Authentication Server Configuration and import the Enterprise Authentication Server's Certificate if necessary.

7. If not done yet, install the latest Service Pack. Refer to [2.31.5 Installing Applications and Service Packs on AW Server in Secured for RMF mode on page 468](#).

#### **NOTE**

We recommend to install the Service Pack before the Secured for RMF activation, because after the activation any Service Pack and Application install will invalidate the RMF mode and activation has to be re-executed.

8. If not done yet, install and activate the required Applications.

Please note that only Volume Viewer applications are supported in Secured for RMF mode

#### **NOTE**

We recommend to install the Applications before the Secured for RMF activation, because after the activation, any Service Pack and Application install will invalidate the RMF mode and activation has to be re-executed.

Proceed to [2.31.3.1 Preparing the Secured for RMF mode on page 452](#).

### **2.31.3.1 Preparing the Secured for RMF mode**

1. Enable the ssh in Service Tools:
  - a. From the Service Tools, select **Tools > Terminal**.
  - b. Click on the SSH **On** button.
2. Prepare the OS installation media, as it may be prompted to mount it during the hardening process (If the latest Service Pack is installed, then in certain cases (Service Pack contains OS updates) RMF activation will not require the media).

For mounting, refer to:

- For Virtual AW Server: [3.10.4.3.2 Virtual AW Server on page 513](#).
- For Physical AW Server: [A.6.2.1 Software load preparation with iLO 5 on page 580](#).

3. Open a terminal and login as **root**.

4. Copy the Hospital central log server's (Syslog server) certificate authority file (`rsyslog_ca.crt` for example) on the local system (the AW Server):

- a. Create a directory where to copy the certificate:

```
mkdir -p /export/home/remoteCA <Enter>
```

- b. Copy the certificate to the AW Server:

```
cd /export/home/remoteCA <Enter>
```

```
scp <Rsyslog server IP>:<Rsyslog server certificate> rsyslog_ca.crt <Enter>
```

- `<Rsyslog server IP>` is the IP address of the Rsyslog server.

- `<Rsyslog server certificate>` is the path to the certificate on the Rsyslog server.

I.e: `scp 3.249.70.244:/etc/pki/tls/certs/ca.crt rsyslog_ca.crt <Enter>`

**NOTE**

Refer to the Customer IT Admin to get the Syslog server IP, the certificate path, the credential and the auditd tcp\_listen port number that will be requested. You can also ask the local IT admin to copy the certificate from his Syslog server to the AW Server.

5. Import all the certificates from the signing chain of the Hospital's central log server's (Syslog server) certificate (except the root CA certificate) into the AW Server:

- a. Gather all the certificate files of all the certificates from the signing chain listed in the Certification Path of the Hospital's central log server's (Syslog server) certificate. Consult the local IT Admin on how to get the certificate files of the certificates from the signing chain.

- b. Upload all the signer certificate files to the AW Server. From the Service Tools, select **Tools > File Transfer**, then select **To System** tab.

The files will be uploaded to the /var/lib/ServiceTools/upload directory.

- c. Open a terminal, login as **root**.

- d. Copy all the uploaded certificate files to the /etc/pki/ca-trust/source/anchors/ directory.

- e. Execute the following command:

**update-ca-trust <Enter>**

6. Import all the certificates from the signing chain (including the root CA certificate) of the Hospital's central log server's (Syslog server) certificate to Certificate Management and configure it for Audit log feature.

**NOTE**

In [Step 4](#) the root CA certificate file was copied to /export/home/remoteCA directory with the name rsyslog\_ca.crt and in [Step 5](#), all other signer certificate files were uploaded to /var/lib/ServiceTools/upload/ directory.

- a. From the Service Tools, select **Administrative > Configuration > Certificate Management**, then select the **Trusted Certificates** tab.

**Follow the next steps for all certificate files.**

- b. Click **Import Third Party Certificate**.

- c. Type in a unique name (for example "rsyslog1") in the **Certificate Name** field.

- d. In **Certificate URL** field, type in the path of the certificate file where it was copied in [Step 5](#) (for example /var/lib/ServiceTools/upload/rsyslog\_ca1.crt).

- e. Click on **Submit** (for the root CA the URL will be for example: /export/home/remoteCA/rsyslog\_ca.crt).

- f. Click **Configure Certificate** button and select the name that was typed previously in [Step 6.c](#) (for example "rsyslog1") in the **Certificates** drop-down menu.

- g. Check **audit log** in the Applications list and click on **Submit**.

Refer to [2.18.11.1 Importing a certificate file to the AW Server trust store on page 212](#) and [2.18.11.2 Associating a certificate with feature\(s\) on page 213](#).

7. Export all the certificates from the signing chain (including the root CA certificate) of the AW Server's certificate to the Hospital's central log server (Syslog server):

If the AW Server is not integrated into the hospital PKI, the Hospital's Syslog server may require some or all the certificates from the signing chain of the AW Server certificate. In that case, ask the local IT admin to copy and export all the needed certificates from the signing chain of the AW Server certificate to the Hospital's central log server (Syslog server).

To get information about the AW Server certificate signer certificates (a.k.a signing chain), refer to [2.18.11.3 Exporting the AW Server certificate file to an external system on page 214](#).

8. Configure Enterprise Repository for Audit Trail (EAT) at **Service Tools > Initial Configuration > Audit Trail (EAT)**. Refer to [2.15.12 Audit Trail \(EAT\) on page 162](#) and perform the “Enterprise Repository case” with TLS connection (select “TLS IETF Syslog” protocol).
9. Configure Time Settings to connect AW Server to the central Time Server (NTP server). The NTP server supplied by the site shall provide a secure connection. It means that it shall be possible to deploy a symmetric key on the NTP server. If it is not the case, the customer IT admin shall provide an NTP server on which a secure connection with a symmetric key can be deployed:
  - a. Configure this NTP server from the Service Tools, select **Initial Configuration > Time Settings** then select the **Time Server** tab. Refer to [2.15.6.2 Time Server menu on page 149](#).
  - b. Ask the customer IT admin to generate a key for the NTP symmetric key scheme authentication and to apply it for their NTP server. Then, to provide the key as a hexadecimal number, the hash method (e.g.: SHA1) and the key ID, which is a decimal number that identifies the key on the NTP server's keystore.

#### NOTE

RMF activation process will install the symmetric key on AW Server. When the Hardening process will ask for the symmetric key, the prefix *HEX:* must be added before the key to sign, it is a hexadecimal number and not a string. (eg.: *HEX:4D59A83F495*).

10. Prepare Kerberos authentication for sending auditd messages from AW Server to the Hospital's central audit log server (auditd):

#### NOTE

This step is optional but required for full RMF compliancy. You can select not to use Kerberos during the activation process resulting in partial RMF compliance.

Ask the customer IT admin to add the necessary licenses to the Kerberos server, generate the keytab file and provide the principal name. Upload the keytab file to the AW Server via Service Tools File Transfer. The Hardening process will ask for the principal name and the path of the uploaded keytab file (/var/lib/ServiceTools/upload is the path where **Service Tools / File Transfer** uploads the files).

11. If not done yet, configure secure connection to all external servers:

#### NOTE

Be aware that Secured for RMF mode enforces TLS1.2 level security. If the external server does not support this, then the connection will not work after RMF activation.

- Audit Trail (EAT): Configure secure TLS connection to the Enterprise Repository entering the details of the Hospital's central log server (Syslog server) and selecting TLS IETF protocol. Also make sure to perform the certificates exchange. See details in [2.15.12 Audit Trail \(EAT\) on page 162](#).
- Configure secure connections (TLS) to the required DICOM hosts and make sure to perform the certificates exchange. See details in [2.18.1 Configuring DICOM hosts in Service Tools on page 184](#).

#### NOTE

DICOM sources without TLS1.2 support can be connected after successful RMF activation. See details in [2.31.3.4 Interoperability with non-RMF compliant systems on page 462](#).

- Configure secure connection (SSL) to the Enterprise Authentication Server with Verify Certificate option switched on and make sure to perform the certificates exchange. See details in [2.18.4 Users \(EA3\) \(User account configuration\) on page 191](#) and [2.18.4.2 Configuring Enterprise User\(s\) Accounts on page 195](#).
  - Optional: In case the Customer uses the Mailsender service, configure secure connection (TLS) to the external SMTP server and make sure to perform the certificates exchange. See details in [2.18.9 MailSender Settings on page 205](#).
12. Optional: Backup configuration, to save this state. Be aware that you can't restore this backup in Secured for RMF mode. The use of this backup is to avoid manual configuration in case of restarting the AW Server installation from scratch.
13. During execution the Hardening process will ask for several detailed information. Before starting the process make sure you have all the information at hand from the below list:

- **GRUB2 password:** You must create a new Bootloader (GRUB2) password.

The following rules apply to GRUB2 password: must be at least 15 characters long, must contain at least one numeric character, must contain at least one uppercase alphabetic character, must contain at least one special character.

#### **NOTE**

Make sure to store this password safely for later use. Refer to [2.21.2 Updating Password\(s\) in Connectivity Database on page 258 Step 1](#).

- **Syslog server IP:** IP address of the Hospital's central log server (Syslog). This is the IP address of the central log server toward which the log messages generated on AW Server are forwarded. Ask IT Admin for this detail.
- **Syslog server port:** syslog port number of the Hospital's central log server (Syslog). Ask IT Admin for this detail.
- **Syslog server common name:** Host name of the Hospital's central log server (Syslog). Ask IT Admin for this detail.
- The path of the Central log server's certificate authority file on the AW Server what you have uploaded earlier in [Step 4](#).
- **Audit log server domain name:** Host name of the Hospital's central audit log server (auditd) towards which the auditd log messages generated on AW Server are forwarded. This can be same or different from the syslog server host name depending on the Hospital's IT architecture. Ask IT Admin for this detail.
- **Auditd tcp\_listen port number:** Port number of the Hospital's central audit log server (auditd). Ask IT Admin for this detail.
- Agree with the IT Admin if you want to enable Kerberos authentication. See [Step 10](#). Based on the decision you have to answer **yes** or **no** to the Kerberos question during install.

#### **NOTE**

In case you have decided not to use Kerberos, make sure that the Kerberos authentication is switched off on the Hospital's central log server too.

- If the decision is to enable the Kerberos authentication, then you will need the:
  - **Path for the file containing the Kerberos key** uploaded to the AW Server in [Step 10](#).
  - **Principal name for Kerberos**
- **Re-authentication time period:** Clarify with the IT Admin if there are any re-authentication time period requirements on Customer side. The time period can be set in days so the most frequent re-authentication time period is daily. In practice this means that after this time period expires, the services sending the logs to the central log

server will restart at midnight, which results in a new authentication when the services re-connect to the log server.

- **NTP server's address:** IP address of the central Time server (NTP). You should have configured by now Time Settings to connect AW Server to the central Time Server (NTP server). See details in [2.15.6 Time Settings on page 148](#).
- **Key for NTP server:** As described in [Step 9.b](#), the IT Admin has to set up NTP symmetric key scheme authentication. IT Admin should provide the generated key before starting the RMF activation.
- **ID of the key:** The ID of the key generated for NTP symmetric key scheme authentication. Ask IT Admin to provide it.

Proceed to [2.31.3.2 Executing the Hardening process on page 456](#).

### 2.31.3.2 Executing the Hardening process

#### NOTE

Be aware that network connections associated with a communication session are terminated by AW Server after 15 minutes of inactivity from the user at a command prompt. If this time-out happens and stops the Hardening execution, you have to start over the Hardening process. So make sure you have all the information and the OS media at hand as described in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 2 and Step 13](#).

#### NOTE

When the Hardening process was already started once on the system even if it was aborted, AW Server will save the answers previously entered, so there is no need to re-enter them. The Hardening process will display the previous answers in square brackets at the end of the question.

Example:

```
dod_installer: Please enter the rsyslog server ip [10.97.226.4]:
```

If you want to enter the same answer, then leave it empty and just press <Enter>.

1. Open a terminal suitable for you to access AW Server through SSH, type the following installer command:

```
bash /usr/local/share/hardening/tools/installer/dod_installer <Enter>
```

The following message appears:

```
dod_installer: Started logging to /var/log/dod_install.log
dod_installer: Important: This can dramatically change your system
behavior! Be careful! These changes cannot be reverted.
dod_installer: Do you really want to fix your system? (yes/no)
```

2. Type:

```
yes <Enter>
```

The following message appears:

```
dod_installer: Is your current AW Server installation a fresh install?
(yes/no)
```

#### NOTE

This question does not appear in case of re-execution of Secured for RMF mode activation after an Application or Service Pack installation.

3. Type:

**yes <Enter>**

**NOTE**

Typing **no** means that the RMF activation will stop and the following message will appear: Installation is aborted, you chose to install RMF mode in a non-supported configuration.

Reason: Currently AW Server does not support upgrade from a non-RMF system or activating Secured for RMF mode on a non-RMF system already in use.

The following message appears:

```
dod_installer: Did you restore any AWS configuration from a non-RMF system? (yes/no)
```

**NOTE**

This question does not appear in case of re-execution of Secured for RMF mode activation after an Application or Service Pack installation.

4. Type:

**no <Enter>**

**NOTE**

Typing **yes** means that the RMF activation will stop and the following message will appear: Installation is aborted, you chose to install RMF mode in a non-supported configuration.

Reason: Currently AW Server does not support upgrade from a non-RMF system.

The following message appears:

```
dod_installer: Have you installed or do you plan to install only supported applications in RMF mode? (For the list of supported applications in RMF mode, please consult the Install Manual.) (yes/no)
```

5. Type:

**yes <Enter>**

**NOTE**

Typing **no** means that the RMF activation will stop and the following message will appear: Installation is aborted, you chose to install RMF mode in a non-supported configuration.

Reason: Currently AW Server supports only Volume Viewer Applications in Secured for RMF mode. Refer to [2.31.2 AW Server Configuration and Limitations in Secured for RMF mode on page 448](#).

The following message appears:

```
dod_installer: Starting with a few interactive questions so the rest of the install can be unattended:  
dod_installer: Please enter the GRUB2 password:
```

6. Type the bootloader (GRUB2) password:

**password <Enter>**

For password rules refer to [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 13](#).

The following message appears:

```
dod_installer: Please retype the password:
```

7. Type the bootloader (GRUB2) password again:

```
password <Enter>
```

The following message appears:

```
dod_installer: Please enter the syslog server ip:
```

8. Type the syslog server IP:

```
<syslog IP> <Enter>
```

The following message appears:

```
dod_installer: Please enter the syslog server port:
```

9. Type the port number of the central log server:

```
<syslog port number> <Enter>
```

The following message appears:

```
dod_installer: Please enter the syslog server common name:
```

10. Type the hostname of the central log server:

```
<syslog server hostname> <Enter>
```

The following message appears:

```
dod_installer: Please enter the path where syslog server's CA is available:
```

11. Type the path where the syslog server's CA is available:

```
/export/home/remoteCA/rsyslog_ca.crt <Enter>
```

This is the location of central log server's certificate authority file that has been copied in the local file system in [2.31.3.1 Preparing the Secured for RMF mode on page 452](#).

The rsyslog\_ca.crt is automatically copied to /etc/pki/rsyslog/rsyslog\_ca.crt.

The following message appears:

```
dod_installer: Please enter the audit log server's domain name
```

12. Type the hostname of the central audit log server for auditd messages provided by the Hospital IT admin. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 13](#):

```
<audit server hostname> <Enter>
```

The following message appears:

```
dod_installer: Please enter the audit log server's tcp_listen port number
```

13. Type the port number of the Hospital's central audit log server (auditd) provided by the Hospital IT admin. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 13](#):

```
<port number> <Enter>
```

The following message appears:

```
dod_installer: Do you want to enable kerberos authentication? Warning, answering 'no' will result in partial RMF compliance! (yes/no):
```

14. Type the answer **yes** or **no** based on the agreement with the Customer. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 13](#):

**NOTE**

In case **no** is answered, make sure that the Kerberos authentication is switched off on the Hospital's central log server too.

The following message appears:

```
dod_installer: Please enter the path for the file containing the  
Kerberos key:
```

15. If **no** was chosen in the previous step then just press <Enter>

In case **yes** was answered then enter the file path where the kerberos key file was uploaded. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 10](#).

The following message appears:

```
dod_installer: Please enter the principal name for Kerberos:
```

16. If **no** was chosen in the [Step 14](#) then just press <Enter>.

In case **yes** was answered then enter the principal name provided by the IT Admin. See details in [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 10](#).

The following message appears:

```
dod_installer: Please enter the services re-authentication time period:
```

17. Type the appropriate time period as agreed with the Customer's IT Admin. The recommended default value is 1. Refer to [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 13](#).

<re-authentication time period> <Enter>

The following message appears:

```
dod_installer: Please enter the NTP server's IP address:
```

18. Type the NTP server's IP address:

<NTP server's IP> <Enter>

This is the IP of the NTP server configured in [2.31.3.1 Preparing the Secured for RMF mode on page 452](#).

The following message appears:

```
dod_installer: Please enter the key for NTP server:
```

19. Type the key for the NTP server with the "HEX:" prefix:

<NTP server's key with prefix> <Enter>

e.g.: HEX:88998EBB469FBB4B151F...

The following message appears:

```
dod_installer: Please enter the ID of the key
```

20. Type the ID of the key:

<ID of the key> <Enter>

The following message appears:

```
dod_installer: Please enter the hash method for the NTP server.
```

21. Type the name of the hash method:

**<Hash method> <Enter>**

The installation continues with the non-interactive steps:

```
dod_installer: Starting DOD mode installation.
dod_installer: The fixes require that the OS CDROM is inserted.
dod_installer: Please insert the OS CDROM and then press enter to
continue...
```

22. Mount the OS installation media, if not done already. If you have already mounted the media as instructed earlier, then the process will automatically continue after some waiting time.

The installation continues with the non-interactive steps:

```
dod_installer: GEHC_SEC_LANG = /home/gehc_security/lang.sh
dod_installer: ### Fri May 27 15:00:57 CEST 2022 # Remove password sync
job from crontab
dod_installer: ### Fri May 27 15:00:57 CEST 2022 # DONE
...
dod_installer: DONE
dod_installer:
=====
dod_installer: Software download Application Uninstallation started
...
dod_installer: Running stigs. This may take some time.
dod_installer: Running V-72083...
...
dod_installer: Running V-72047...
...
dod_installer: All 181 stig fixes have been run.
...
System will reboot automatically in 3 minutes. Press Enter to manually
reboot... Remaining time: 140 seconds.
```

23. It takes several minutes (~15 minutes) and two reboots to complete the DOD installer process.

The DOD installer process is completed once the Service Tools is reachable.

Press **<Enter>** to reboot the AW Server.

In case it is needed to repeat the execution, values once entered will be available as defaults.

On successful completion, Secured for RMF mode is indicated in the HealthPage of Service Tools.

Automatic Configuration Status Summary	N/A
Secured for RMF	On
RMF activation date	2020-04-30 11:13:52.659444805 +0200
RMF verification date	N/A
Refresh	

24. To finalize the hardening process, open a terminal, login as **root**.

The hardening recommendations display (same recommendations as in the Service Tool login capture below in this section).

25. To finalize the hardening process, execute the finalizer process script:

**bash /usr/local/share/hardening/tools/installer/dod\_finalizer <Enter>**

The following message appears:

```
dod_finalizer: Started logging to /var/log/dod_install.log
dod_finalizer: Freezing baseline...
dod_finalizer: Running dod_verifier...
```

```

...
dod_finalizer: Running /usr/local/share/hardening/stigs/RHEL7/checks/
V-72127 ...ok
...
dod_finalizer: Running /usr/local/share/hardening/stigs/RHEL7/checks/
V-72047 ...ok
dod_finalizer: All 200 tests passed. [ OK ]
...
dod_finalizer: Finished verifying DOD mode installation.
dod_finalizer: Stopping logger
dod_finalizer: Finished finalizing DOD mode installation.
dod_finalizer: Stopping logger

```

26. Press <Enter> to exit the finalizer script.

Proceed to [2.31.3.3 Finalizing configuration after Secured for RMF Mode activation on page 461](#).

### 2.31.3.3 Finalizing configuration after Secured for RMF Mode activation

1. Make sure you are still in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
2. Update the McAfee Virus Database and engine. Refer to [2.31.6 McAfee Virus Database update on page 469](#).
3. Change the passwords:
  - a. **Linux:** Change **root** password manually using a command line window. Refer to [2.21.1.2 Changing Linux passwords on page 251 Step 2.c](#).

**Important**

Make sure to store the password safely for later use Refer to [2.21.2 Updating Password\(s\) in Connectivity Database on page 258 Step 1](#).

- b. **EA3:** Change the **service** user password. Refer to [2.18.4 Users \(EA3\) \(User account configuration\) on page 191](#) and [2.31.10 Local password policy in Secured for RMF mode on page 478](#).

**Important**

Make sure to store the **service** password safely for later use Refer to [2.21.2 Updating Password\(s\) in Connectivity Database on page 258 Step 1](#).

- c. **EA3:** For all other existing local users set **Change Password on Next Login** check box. Refer to [2.18.4 Users \(EA3\) \(User account configuration\) on page 191](#).
4. If User Management is not performed via an Enterprise Server (which means that the system will be only partially RMF compliant), then create the required local users. Refer to [2.18.4 Users \(EA3\) \(User account configuration\) on page 191](#).

**Important**

For all newly created local users set **Change Password on Next Login** check box.

5. **Optional:** Configure DICOM exceptions for VNAs not supporting TLS. Refer to [2.31.3.4 Interoperability with non-RMF compliant systems on page 462](#).
6. Review and check the configuration of all DICOM Hosts defined prior enabling RMF mode (e.g.: port must be the TLS port) Use "Check DICOM" to verify the configuration. Refer to [2.18.1 Configuring DICOM hosts in Service Tools on page 184 Step 6 to Step 8](#).
7. Backup configuration. Refer to [2.28.2.2 Configuration Backup on page 303](#).

8. Explain to IT Admin the DoD requirement of regular backups and how to do it:
  - According to DoD policies backup shall be done at regular intervals and these backups should be stored offsite with appropriate physical and technical protection. See [2.31.2 AW Server Configuration and Limitations in Secured for RMF mode on page 448](#).
  - The IT Admin can get a backup for this purpose via **Service Tools > Maintenance > Backup > System configuration** using the **Pull from System** command.
  - Explain the IT Admin that to fulfill this DoD requirement he has to perform this operation and transfer the backup file to the safe location regularly.
  - Inform the IT Admin that the instructions are also available in the *Admin Guide in Chapter 7.5.4.1 Backing up system configuration*.
9. Register configuration. Refer to [2.31.3.5 Configuration registration solution in RMF \(DoD mode on page 465\)](#).
10. Finish Maintenance mode. Refer to [A.4.2 Exiting the Maintenance mode on page 573](#).
11. Verify Secured for RMF mode. Refer to [2.31.3.6 Verifying the Secured for RMF Mode on page 466](#).
12. Perform Server Installation Validation Tests. Refer to [2.23 Job Card IST014 - Server Installation Validation Tests on page 263](#).

### 2.31.3.4 Interoperability with non-RMF compliant systems

In RMF mode all non-local connections must be encrypted to protect the confidentiality of remote access sessions and also appropriate cryptographic mechanisms must be implemented for them to protect their integrity. To comply with these requirements remote access sessions are secured in RMF mode. This is typically implemented through TLS. In case of special cases when the site has non-RMF compliant VNA's then AW Server provides a compatibility script which can be used to temporarily enable unsecure connections for interoperability until the site manages to provide fully RMF compliant VNA's. These cases must be evaluated by the site and these RMF exceptions must be noted.

In case if unsecure connections are agreed to be used temporarily the FE can use the compatibility script on AWS:

Name:

`dicom_host_secure.setter`

Full path on the AW Server:

`/usr/local/share/hardening/tools/dicom_host_secure.setter`

Params:

- **dicom\_host\_name**: The name of the DICOM host, what you given in Service Tools.
- **secure\_value**: Value must be true or false. This value will be set for Secure tag in the network-cfg.xml file.

Example for enabling unsecure the connection for DICOM host `dicom-host-1: # /usr/local/share/hardening/tools/dicom_host_secure.setter dicom-host-1 false`

Example for enabling re-securing the connection for DICOM host `dicom-host-1: # /usr/local/share/hardening/tools/dicom_host_secure.setter dicom-host-1 true`

So the configuration procedure is the following assuming that the host name of the DICOM host is "dicom-host-1":

1. Make sure you are still in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

2. Configure the DICOM host like it would be capable to do secure connection. Refer to [2.18.1 Configuring DICOM hosts in Service Tools on page 184](#).

Do not test the DICOM connection yet, just enter the required values:

**DICOM Host Access Control** Maintenance mode required!

Only hosts in this list       Any host  
Recommended      Any host is allowed to C-FIND and C-STORE.

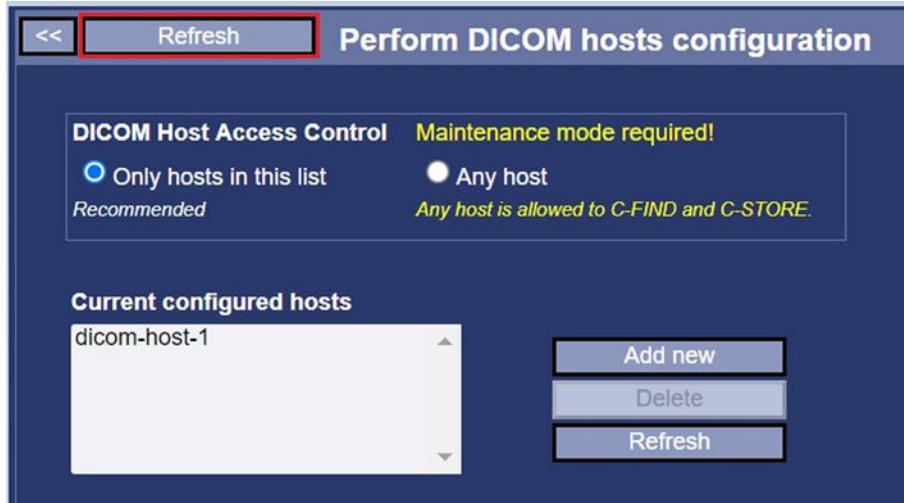
**Current configured hosts**

Name*	dicom-host-1
Host name*	dicom-host-1
Application Entity Title*	dicom-host-1
IP address*	10.97.226.84
<input type="button" value="Check IP"/>	
Encrypted (TLS)	<input checked="" type="checkbox"/>
Port*	2762
<input type="button" value="Check DICOM"/>	
Query/retrieve supported	<input checked="" type="checkbox"/>
Custom Search	<input type="checkbox"/>

3. If not done yet, enable SSH. From the Service Tools, select **Tools > Terminal** and set **SSH** to **On**.
4. Open a terminal suitable for you to access AW Server through SSH and log in as **root** user to the AW Server.
5. In the terminal run the exception script:

```
# /usr/local/share/hardening/tools/dicom_host_secure_setter dicom-host-1
false
```

6. Go back to the Service Tools and select **Administrative > Configuration > DICOM Hosts**. Click the **Refresh** button on the top of the page.



7. Select the created DICOM host again from the **Current configured host** list.
8. Now the **Encrypted (TLS)** checkbox is unchecked and you can finalize the configuration with an unsecure connection. Leave the **Encrypted (TLS)** checkbox unchecked.
9. Change the **Port\*** value to the non-TLS value:
  - **4006** for AW Server DICOM
  - **104** for Enterprise Archive DICOM

Name*	dicom-host-1
Host name*	dicom-host-1
Application Entity Title*	dicom-host-1
IP address*	10.97.226.84
Check IP	
Encrypted (TLS)	<input type="checkbox"/>
Port*	4006
Check DICOM	

10. Finish the configuration of the DICOM host and test the connection. Refer to [2.18.1 Configuring DICOM hosts in Service Tools on page 184](#).
11. Do not forget to click **Apply** after finishing the configuration.

C-MOVE instance level threshold	100000	Use defa
C-FIND cancellation strategy	AsyncAbort	Use defa
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

12. Disable SSH and exit Maintenance mode if you do not plan to do any other configuration operation.

### 2.31.3.5 Configuration registration solution in RMF (DoD) mode

In Secured for RMF mode the Register Configuration UI is disabled. Configuration registration can be performed using command line solution.

Command line based Configuration Registration procedure:

Make sure you are in Maintenance mode before start. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

#### 1. Export configuration

- a. Open a terminal suitable for you to access AW Server through SSH and log in as **root** user to the AW Server.

Please use the following command to generate the conf file:

```
/usr/share/icm/icm.sh --generateConf /tmp/
```

The command will return the path of the generated Configuration file:

```
/tmp/<licenseID>_<SystemID>_<DateTime>_Configuration.txt
```

- b. Copy the generated Configuration file to your PC or to a media (e.g. USB stick).

#### 2. Register configuration and retrieve the registration key

- a. Launch an Internet Navigator and connect to <https://awcct.gehealthcare.com>.
- b. Click on the **Choose File** button on the **AW Configuration Collection Tool** page, then select your AW Server's Configuration file. Click on **Submit**.

The AW Configuration Collection Tool screen displays the Summary of uploaded Configurations.

If the configuration is compliant, you will get your system Registration key.

- c. Click on **Save registration Key** button, and choose the location where to save the key on your PC.

#### 3. Install registration key on AW Server

- a. Open again the command line and use the following command - adding the registration key in place of <registration\_key> argument:

```
/usr/share/icm/icm.sh --setkey <registration_key>
```

The command will result the following output:

```
The registration key has been successfully installed
```

- b. To ensure that the configuration registration is successful you may issue the following command:

```
/usr/share/icm/icm.sh --status
```

This command should output the following result:

```
Registration Key: <registration_key>
```

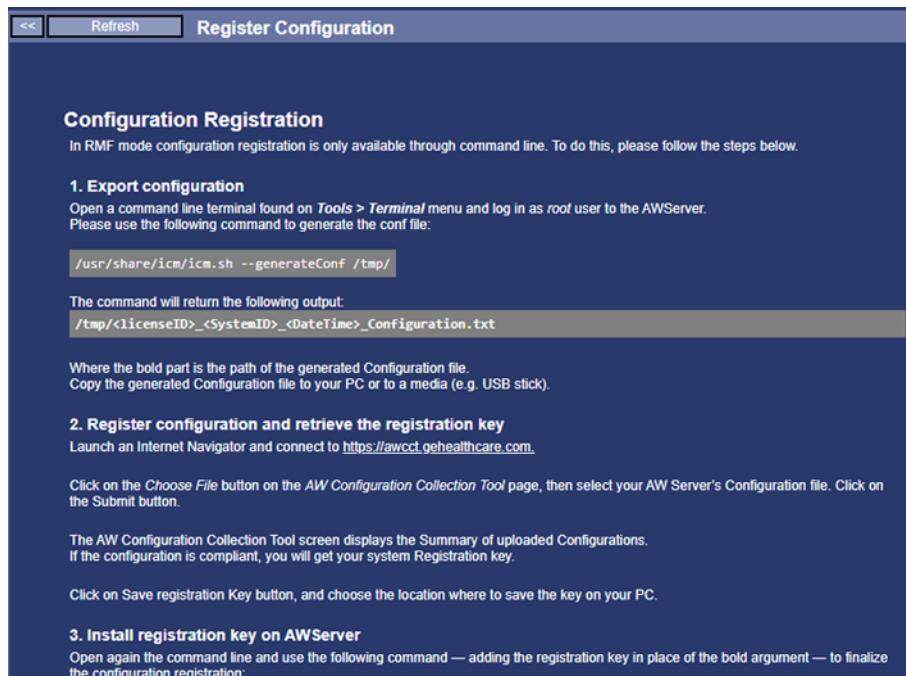
```
Registration Status: Standard
```

Where the <registration\_key> should be identical to the one you have received from AWCCT site.

- c. Finish Maintenance mode. Refer to [A.4.2 Exiting the Maintenance mode on page 573](#).

#### NOTE

The instructions are also visible in place of the Register Configuration UI. From the Service Tools, select **Maintenance > Register Configuration**.

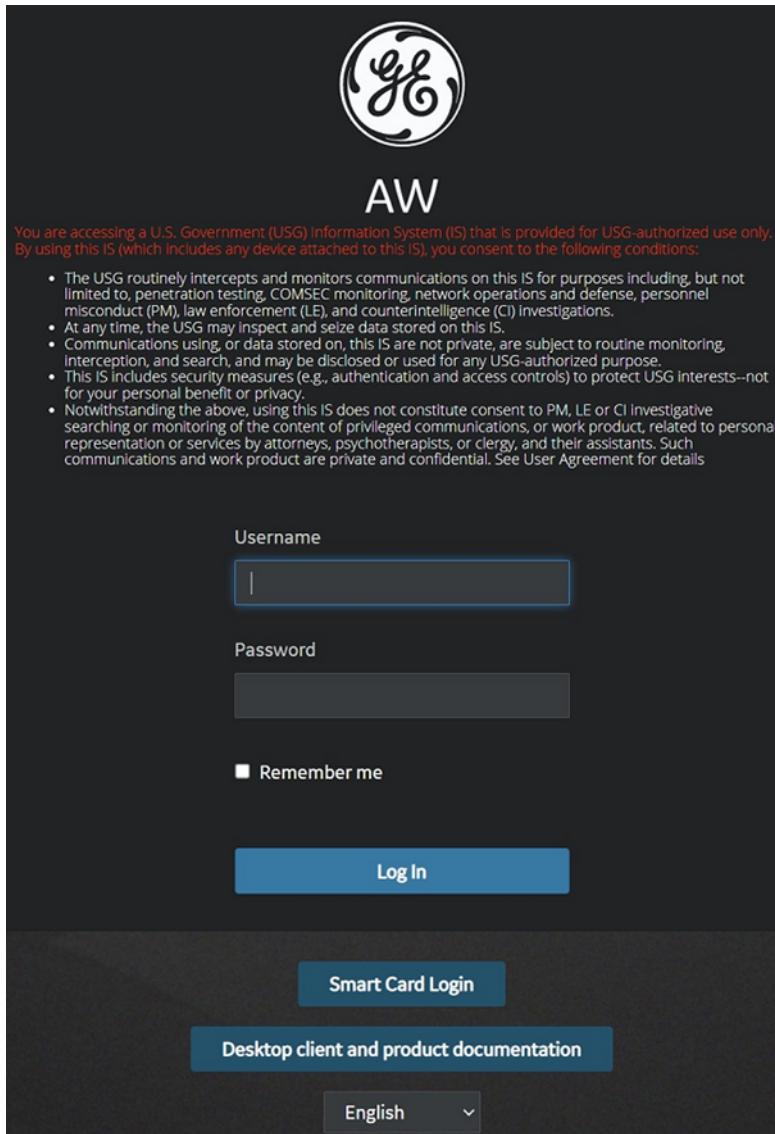


### 2.31.3.6 Verifying the Secured for RMF Mode

To verify the Secured RMF Mode is activated, check the following:

1. Logout from the Service Tools and login again.

When login into Service Tools, check the hardening recommendations appear:



## 2. Check the HealthPage:

- If the RMF status is displayed as below, then it means that RMF mode is activated and verified (after successful run of `dod_installer` and `dod_finalizer` commands):

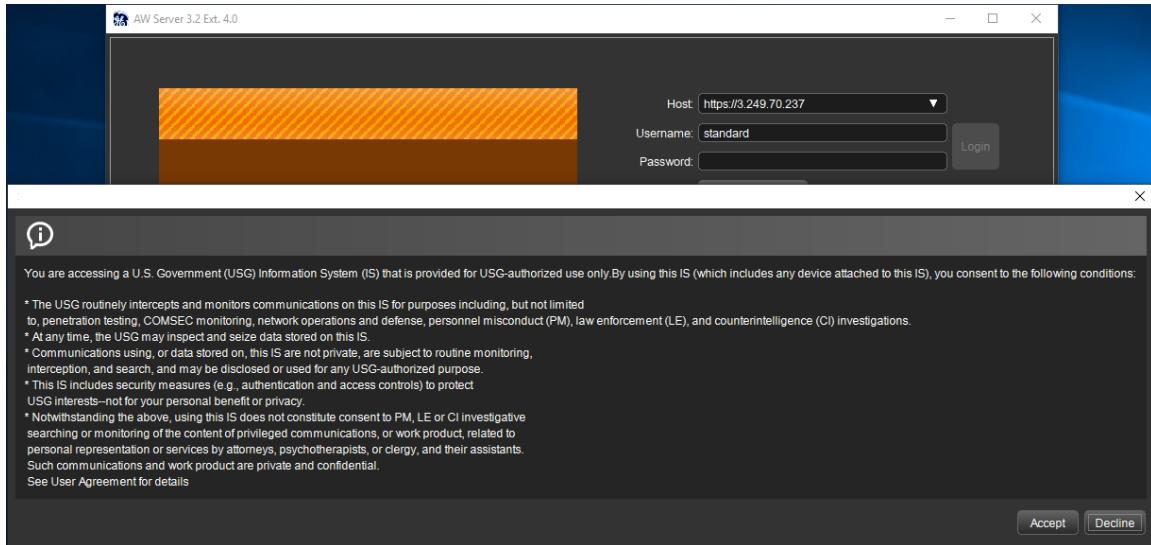
Summary	
Secured for RMF	On, verified
RMF activation date	2020-04-30 11:13:52.659444805 +0200
RMF verification date	2020-05-06 18:49:40.591468093 +0200
Refresh	

- Right after Application or Service Pack installation, the status will display:

Secured for RMF	On
RMF activation date	2022-10-24 12:19:20.036463382 +0200
RMF verification date	N/A

In this case `dod_finalizer` must be re-executed to achieve to the fully verified RMF status. Refer to [2.31.5 Installing Applications and Service Packs on AW Server in Secured for RMF mode on page 468](#).

3. When login into the AW Server Client, check the hardening recommendations appear:



4. Check the connectivity to the hospital central log server:
  - a. Open a terminal, login as **root**.
  - b. Contact the Customer IT Admin to check that the hospital Rsyslog server received the login access.

## 2.31.4 Upgrading an AW Server in RMF mode

There is no tested upgrade path to **AWS3.2 ext4.9** in Secured for RMF mode. There is no direct upgrade procedure from earlier non-RMF releases or from earlier engineering releases where RMF was activated to **AWS3.2 Ext. 4.9** release with Secured for RMF mode activated. We recommend installing a new **AWS3.2 Ext. 4.9** server, configure it manually and activate Secured from RMF mode, just like in case of a fresh installation.

## 2.31.5 Installing Applications and Service Packs on AW Server in Secured for RMF mode

### Important

After installing Applications or Service Packs on AW Server in Secured for RMF mode, system's compliance with RMF requirements is no longer verified on the server.

Therefore, after a successful install the FE must re-execute the Secured for RMF mode verification again.

### NOTE

Only Volume Viewer applications are supported in secured for RMF mode

### NOTE

Make sure that you install the latest Service Pack for the particular AW Server. When installing from electronic files, always refer to *AW eDelivery Service Guide 5761599-8EN* for detailed instructions.

### NOTE

Secured for RMF mode allows to upload only signed packages to the AW Server.

To install Applications or a Service Pack, please perform the following steps:

1. Activate Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

2. Install the Applications or the latest Service Pack on the AW Server. Refer to [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#) and [3.10.4.5 OS and AW Server Platform software Service Pack installation on page 518](#).
3. After successful installation, go to the Healthpage on Service Tools. The Secured for RMF status is On but marked with yellow background and the RMF verification date deleted:

Secured for RMF	On
RMF activation date	2022-10-24 12:19:20.036463382 +0200
RMF verification date	N/A

4. Open a terminal to access AW Server through SSH, login as **root** and run `dod_finalizer`. Refer to [2.31.3.2 Executing the Hardening process on page 456, Step 25](#).
5. Backup configuration. Refer to [2.28.2.2 Configuration Backup on page 303](#).
6. Register configuration. Refer to [2.31.3.5 Configuration registration solution in RMF \(DoD\) mode on page 465](#).
7. Finish Maintenance mode. Refer to [A.4.2 Exiting the Maintenance mode on page 573](#).
8. Perform Server Installation Validation Tests. Refer to [2.23 Job Card IST014 - Server Installation Validation Tests on page 263](#).
9. Test the newly installed application if any.

## 2.31.6 McAfee Virus Database update

Antivirus softwares requires regular update to maintain up to date protection against the latest security threats. For McAfee this means that the antivirus database, the so called Virus Definition Update (DAT) and the antivirus engine of the software requires regular check for updates and if new version is available, that has to be installed on AW Server. RMF installations are not connected to the public Internet, so this update has to be performed manually.

The Field Engineer must do the update procedure at the initial installation and check for updates whenever he is on site. Subsequently the Customer IT Admin has to do the procedure whenever there is an update available.

To perform the update follow the bellow procedure:

## 2.31.6.1 Antivirus Database and engine update check

- From the Service Tools, select **Maintenance > Antivirus**.

**Antivirus database update**

- Download the latest Virus Definition Update (DAT) from the McAfee website on your laptop.
  - Go to URL - <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>
  - Navigate to ".DATs" tab.
  - Download the "DAT Package For Use with McAfee ePO" package under "Download MEDDAT Updates" title.
- Extract the package and upload it to the AW Server.
  - Extract the file named "mediumdat-[DAT number].zip" from the downloaded DAT Package (mediumepoXXXXdat.zip).
  - Upload the extracted file to the AW Server via the below "Upload DAT package" button.
  - After successful upload, copy the file path to the clipboard.
- Update the antivirus database on the "McAfee Endpoint Security for Linux Threat Prevention [ENSLTP]" tool below.
  - Note: Ignore the instructions displayed by the tool.
  - Navigate to "Antivirus non-ePO setup" tab.
  - Paste the file path of the uploaded file from the clipboard to the "Enter DAT/Engine location:" field.
  - Press "Update dat" button.

**Upload DAT package** File path:

**Antivirus engine update**

- Download the latest antivirus engine updates from the McAfee website on your laptop.
  - Go to URL - <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>
  - Navigate to "Engines" tab.
  - Download the package "Linux Engine Package for Use with ePO".
- Extract the package and upload it to the AW Server.
  - Extract the file named "avengine64.zip" from the downloaded Linux Engine Package (ePOxxxxlnx.zip).
  - Upload the extracted file to the AW Server via the below "Upload engine package" button.
  - After successful upload, copy the file path to the clipboard.
- Update the antivirus engine on the "McAfee Endpoint Security for Linux Threat Prevention [ENSLTP]" tool below
  - Note: Ignore the instructions displayed by the tool.
  - Navigate to "Antivirus non-ePO setup" tab.
  - Paste the file path of the uploaded file from the clipboard to the "Enter DAT/Engine location:" field.
  - Press "Update engine" button.

**Upload engine package** File path:

- Ignore the instruction text at the top of the page for now.
- Scroll down to the bottom of the page to reach the **McAfee Endpoint Security for Linux Threat Prevention [ENSLTP]** page.
- On the first tab called **Antivirus scan** check the data in the top section called **Antivirus details**.
- Note the values at **Engine version** and **DAT file version**.

<b>Antivirus details</b>	
Antivirus version	: 10.7.10.62
Engine version	: 6400.9594
DAT file version	: 999.0

- Go to URL <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>.

- On the web page first select the **.DATs** tab and check the **Version** value in the **Download MEDDAT Updates** table.

**Security Updates**

**DATs**   **Engines**   **Content**

LANGUAGE English

Download V2 Virus Definition Updates (DATs)

Download MEDDAT Updates

DAT File	Platform	Notes	Version	Release Date	File Size (MB)
DAT Package For Use with McAfee ePO	Linux and Mac		5001	06/12/2022	89.34

- If this value is bigger than the **DAT file version** value in the **Antivirus Details** section then go to [2.31.6.2 Antivirus Database Update on page 471](#) and perform the update.
- Go back to the web page and select the **Engines** tab and check the **Version** value in the **Download Engine Updates** table at the **Linux Engine Package for Use with ePO** row.

**Security Updates**

**DATs**   **Engines**   **Content**

Download Engine Updates

Download Engine Updates

Product	Platform	Notes	Version	Release Date	File Size (MB)
epo6400eng.zip Windows Engine Package for use with ePO	Windows	<a href="#">Release Notes</a>	6400	12/14/2021	5.83
epo6400mub.zip Mac OS Universal Engine Package for use with ePO	Mac OS	<a href="#">Release Notes</a>	6400	12/14/2021	7.27
epo6400lnx.zip Linux Engine Package for use with ePO	Linux	<a href="#">Release Notes</a>	6400	12/14/2021	6.99

- If this value is bigger than the **Engine version** value in the **Antivirus Details** section then go to [2.31.6.3 Antivirus Engine Update on page 474](#) and perform the update.

## 2.31.6.2 Antivirus Database Update

### NOTE

AW Server does not have to be in Maintenance mode during this operation, but it is recommended to do this operation during maintenance period.

- Download the latest Virus Definition Update (DAT) from the McAfee website on your laptop.
  - Go to URL - <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>.

- b. Navigate to **.DATs** tab.

The screenshot shows a web interface titled "Security Updates". At the top, there is a navigation bar with three tabs: ".DATs" (which is highlighted with a red box), "Engines", and "Content". Below the navigation bar, there is a language selection dropdown set to "English". The main content area contains the text "Download V2 Virus Definition Updates (DATs)".

- c. Download the **DAT Package For Use with McAfee ePO** package under **Download MEDDAT Updates** title.

#### Download MEDDAT Updates

DAT File	Platform	Notes	Version	Release Date	File Size (MB)
<a href="#">DAT Package For Use with McAfee ePO</a>	Linux and Mac		5001	06/12/2022	89.34

2. Extract the package and upload it to the AW Server.

- a. Extract the file named `mediumdat-[ DAT number ].zip` from the downloaded DAT Package (`mediumepoxXXxdat.zip`).
- b. In the **Antivirus** page, click on **Upload DAT package** button.

**Upload DAT package** File path: /var/lib/ServiceTools/upload/antivirus/mediumdat-5002.zip

- c. Upload the extracted file to the AW Server, using the **Send files to systems** popup that displays.

#### NOTE

Be aware that the **Send files to system** dialog always appears at the top of the page over the **Antivirus database update** instructions. Scroll up if you do not see the dialog.

#### Antivirus database update

The dialog box has the following steps:

1. Download the latest Virus Definition Update (DAT) from the McAfee website on your laptop.
  - Go to URL - <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>
  - Navigate to ".DATs"
  - Send files to system (files are stored under /var/lib/ServiceTools/upload/antivirus)**
2. Extract `mediumdat-[ DAT number ].zip` (optional)
  - `md5 or sha-1 checksum (optional)`
  - 
  - Choose File** No file chosen
3. Update
  - Send to system**
  - Cancel**

On the right side of the dialog, there is a note: "IDAT Updates" tip: If you have already extracted the DAT file, you can skip this step and use the "Send files to system" tool below the dialog. The "Send files to system" tool is located in the "mediumepoxXXxdat.zip" file, which is part of the DAT package. You can find it by navigating to the "SLTTP" tool below the dialog.

- d. Copy the file path, that appears next to the **Upload DAT package** button, into the clipboard.
- 3. Update the antivirus database on the **McAfee Endpoint Security for Linux Threat Prevention [ENSLTP]** tool below.

- a. Navigate to **Antivirus non-ePO setup** tab.

#### NOTE

Ignore the instructions displayed by the tool.

**Antivirus details**

- Antivirus version : 10.7.10.62
- Engine version : 6400.9594
- DAT file version : 999.0

**Instructions to update DAT / Engine packages**

- Download the latest Virus Definition Update (DAT) and antivirus engine packages:
  - Go to URL – <https://www.treliix.com/en-us/downloads/security-updates.html>
  - Engine: Navigate to "Engines" tab and download the package "Linux Engine Package for Use With ePO"
  - DAT: Navigate to ".DATs" tab and download the package "DAT Package For Use with McAfee ePO" under "Download MEDDAT Updates" title.
- Extract the package and copy the files:

- Paste the file path of the uploaded file from the clipboard to the **Enter DAT/Engine location:** field.
- Press **Update DAT** button and wait till the **Status information** shows Antivirus DAT successfully updated message.

Select USB

Select DAT/Engine file

OR

Enter DAT/Engine location: `/var/lib/ServiceTools/upload/antivirus/mediumdat-`

**Status information**

**Update DAT**

**Update Engine**

**Status information**

Antivirus DAT is updating  
Antivirus DAT successfully updated

- On the top of the tab in the **Antivirus Details** section you can see the updated DAT file version.

**Antivirus details**

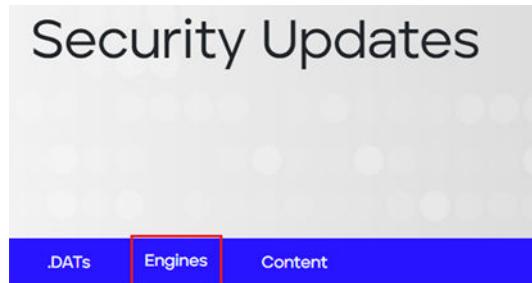
- Antivirus version : 10.7.10.62
- Engine version : 6400.9594
- DAT file version : 999.0

## 2.31.6.3 Antivirus Engine Update

### NOTE

AW Server does not have to be in Maintenance mode during this operation, but it is recommended to do this operation during maintenance period.

1. Download the latest antivirus engine updates from the McAfee website on your laptop.
  - a. Go to URL - <https://www.mcafee.com/enterprise/en-us/downloads/security-updates.html>.
  - b. Navigate to **Engines** tab.



Download Engine Updates

- c. Download the **Linux Engine Package For Use with ePO**.

Download Engine Updates

Product	Platform	Notes	Version	Release Date	File Size (MB)
<a href="#">epo6400eng.zip</a> Windows Engine Package for use with ePO	Windows	<a href="#">Release Notes</a>	6400	12/14/2021	5.83
<a href="#">epo6400mub.zip</a> Mac OS Universal Engine Package for use with ePO	Mac OS	<a href="#">Release Notes</a>	6400	12/14/2021	7.27
<a href="#">epo6400inx.zip</a> Linux Engine Package for use with ePO	Linux	<a href="#">Release Notes</a>	6400	12/14/2021	6.99

2. Extract the package and upload it to the AW Server.

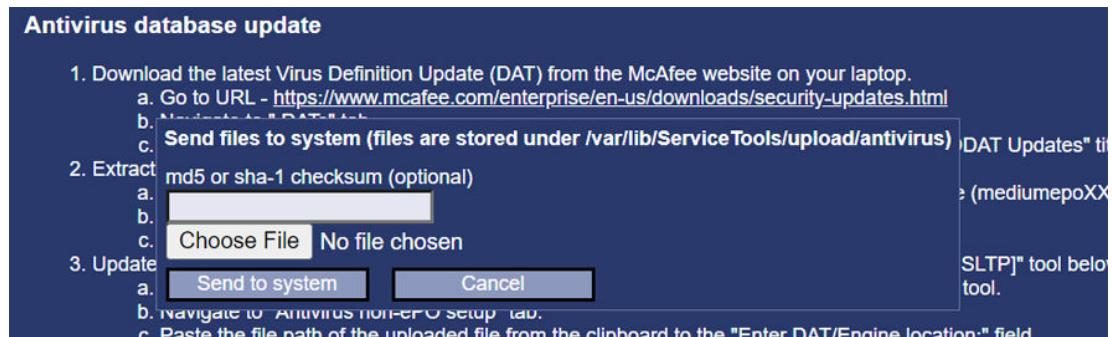
- a. Extract the file named `avengine64.zip` from the downloaded Linux Engine Package (`ePOxxxxInx.zip`).
- b. In the **Antivirus** page, click on **Upload DAT package** button.



- c. Upload the extracted file to the AW Server, using the **Send files to systems** popup that displays.

### NOTE

Be aware that the **Send files to system** dialog always appears at the top of the page over the **Antivirus database update** instructions. Scroll up if you do not see the dialog.



- d. Copy the file path, that appears next to the **Upload DAT package** button, into the clipboard.
- 3. Update the antivirus engine on the **McAfee Endpoint Security for Linux Threat Prevention [ENSLTP]** tool below.
  - a. Navigate to **Antivirus non-ePO setup** tab.

#### NOTE

Ignore the instructions displayed by the tool.

**Antivirus scan** **Antivirus non-ePO setup**

**Antivirus details**

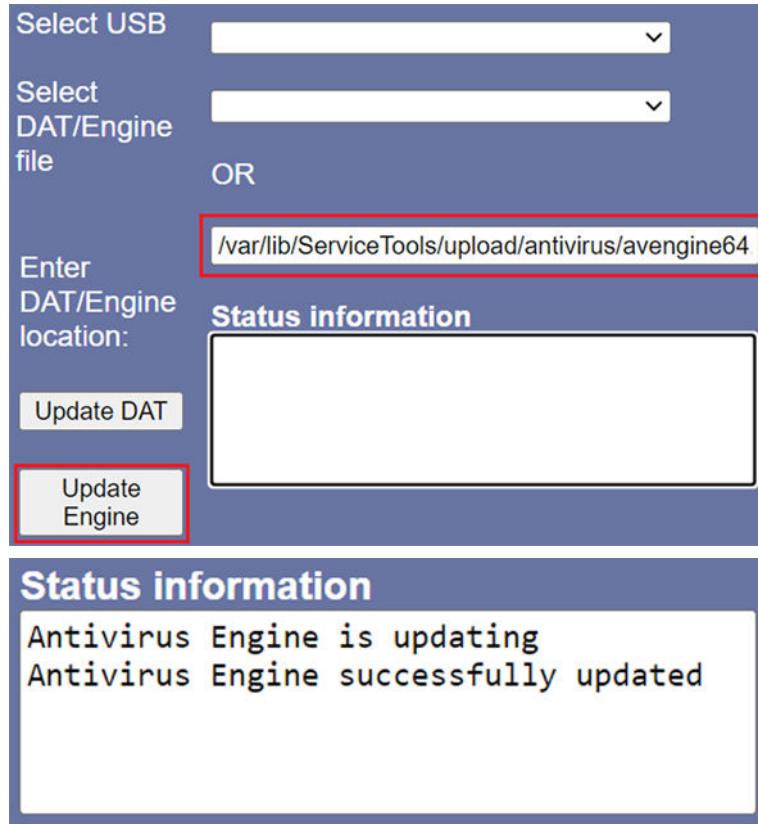
Antivirus version	:	10.7.10.62
Engine version	:	6400.9594
DAT file version	:	999.0

**Instructions to update DAT / Engine packages**

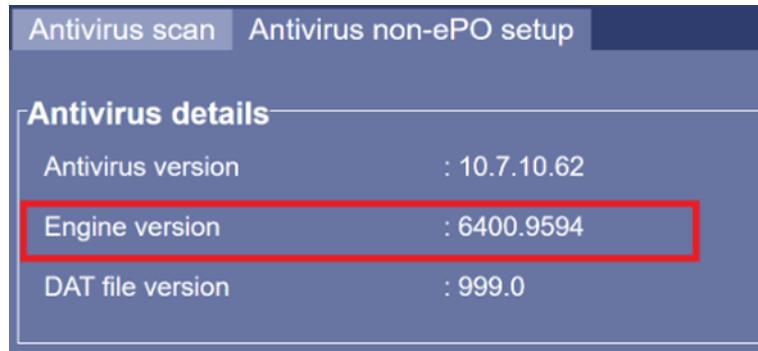
1. Download the latest Virus Definition Update (DAT) and antivirus engine packages:
  - a. Go to URL – <https://www.trellix.com/en-us/downloads/security-updates.html>
  - b. Engine: Navigate to "Engines" tab and download the package "Linux Engine Package for Use With ePO"
  - c. DAT: Navigate to ".DATs" tab and download the package "DAT Package For Use with McAfee ePO" under "Download MEDDAT Updates" title.
2. Extract the package and copy the files:

- b. Paste the file path of the uploaded file from the clipboard to the **Enter DAT/Engine location:** field.

- c. Press **Update Engine** button and wait till the **Status information** shows Antivirus Engine successfully updated message.



- d. On the top of the tab in the **Antivirus Details** section you can see the updated Engine version.



## 2.31.7 Troubleshooting the Secured for RMF mode

Please be aware that the Secured for RMF activation is **an irreversible process**. There is no roll-back to original state in case of successful execution or in case of any errors.

If there are any issues during the execution of the Secured for RMF Mode Installer Script (`dod_installer`), the script stops with the appropriate error message. The system will be in a transient state where parts of the RMF changes were executed and parts were not. The events are logged into the file `/var/log/dod_install.log`.

In this case, the installation of the Secured for RMF mode has failed.

- In case of simple errors (i.e.: provided a wrong answer to the initial questions or mounted the wrong iso file as OS CDROM), then simply re-start the RMF Mode Installer Script (`dod_installer`).

- In more complex error situation, please contact your local Online Center to diagnose the issues.

### Known issues

#### Problem:

In case the `dod_installer` executed successfully, but `dod_finalizer` returned the following error:

```
dod_finalizer: test_framework::assert_true "check_alive_chrony_connections" "Chrony is using an unauthorized source"
dod_finalizer: Running /usr/local/share/hardening/stigs/APPSECDEV/checks/V-70245 failed
```

Then most probably wrong values have been entered for the NTP server security settings in the initial questionnaire: key for the NTP server, ID of the key and name of the hash method. Refer to [2.31.3.2 Executing the Hardening process on page 456 Step 19, Step 20 and Step 21](#).

#### Solution:

1. Double check the NTP Server settings with the IT Admin. Refer to [2.31.3.1 Preparing the Secured for RMF mode on page 452 Step 9](#).
2. Re-execute the hardening process starting from [2.31.3.2 Executing the Hardening process on page 456 Step 1](#) and **carefully** to enter the **correct** NTP server values.

## 2.31.8 Changing AW Server configuration in Secured for RMF mode

In all cases after changing the configuration of AW Server in secured for RMF mode, always perform the RMF verification to make sure that RMF compliance is still valid. The verification of the compliance can be tested only after finishing Maintenance mode as the `dod_verifier` script tests the production environment. If the `dod_verifier` script fails, then it means that the configuration changes did break the RMF compliance. In that case, FE has to re-enter Maintenance mode and re-activate the Secured for RMF mode.

#### NOTE

Configuration changes do break RMF compliance quite often. Re-activating Secured for RMF mode after a configuration change is considered standard procedure.

After the configuration changes are done, the FE has to do the following steps:

1. Do not exit Maintenance mode.
2. Open a terminal suitable for you to access AW Server through SSH and log in as `root` user to the AW Server. Keep this SSH connection open through the entire process.
3. Register the configuration. Refer to [2.31.3.5 Configuration registration solution in RMF \(DoD\) mode on page 465](#).
4. Finish Maintenance mode, but keep the SSH session open.

#### NOTE

In normal production mode when Secured for RMF is activated, AW Server does not allow to start an SSH session. But SSH sessions started during Maintenance mode will be still working.

5. Execute the `dod_verifier` script in the terminal:

```
bash /usr/local/share/hardening/tools/installer/dod_verifier <Enter>
```

6. In case of successful verification, the following message appears:

```
dod_verifier: Started logging to /var/log/dod_install.log
dod_verifier: Verifying DOD mode installation.
...
dod_verifier: Running /usr/local/share/hardening/stigs/RHEL7/checks/
V-72127 ...ok
...
dod_verifier: All 200 tests passed. [ OK ]
dod_verifier: Finished verifying DOD mode installation.
dod_verifier: Stopping logger
```

In this case the **dod\_verifier** script found that the AW Server RMF compliance is still valid. That means that the system can be safely used for production.

7. In case of failed verification, the output of **dod\_verifier** script will contain the following lines at the end:

```
dod_verifier: Failures found!
dod_verifier: Error: Verifying the DOD installation failed. Revise your
system, fix it and run 'dod_install' again to complete the dod
installation.
```

In this case, re-enter Maintenance mode, correct the system (please contact your local Online Center to diagnose the issues) and re-execute the Hardening process starting from [2.31.3.1 Preparing the Secured for RMF mode on page 452](#). Once the RMF verification was successful FE has to register the changed configuration before exiting the Maintenance mode. Refer to [2.31.3.5 Configuration registration solution in RMF \(DoD\) mode on page 465](#).

## 2.31.9 Account Authentication Policies

### 2.31.9.1 Linux Accounts

The operating system is configured to lock accounts for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe. The operating system is configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds. Do not use the **authconfig** tool in the operating system for authentication configuration, it may overwrite the system hardening settings.

#### NOTE

This fail lock mechanism does not apply to the **root** Linux user account

### 2.31.9.2 AW Server User Accounts

The AW Server is configured to lock accounts for a minimum of 15 minutes after three unsuccessful logon attempts.

## 2.31.10 Local password policy in Secured for RMF mode

If not already done while installing/upgrading the AW Server, the default passwords should be changed. Follow the steps described in [2.21 Job Card IST006 - Changing the Passwords on page 249](#). In addition to the password strength rules detailed in [2.21.1.1 Identify New Password\(s\) on page 250](#), the following password/account related rules apply to the system after running the Secured for RMF mode installer script:

- When changing a password:
  - At least 8 characters must be changed.
  - At least 4 character classes must be changed.
  - The number of repeating characters of the same character class must not be more than four characters.

- Prohibit the reuse of passwords within 5 iterations.
- Force user to change passwords at least every 60 days.
- Prevent users to change passwords more than once every 24 hours.
- Require password to edit the boot menu or to boot into single user mode.

If existing local users do not change their password at RMF installation time, the system will ask to change the password after 60 days.

If users change their password, only the password strength is applied to the new password.

If a new local user is created then all rules apply and the password must be changed every 60 days.

## 2.31.11 Checking RMF mode integrity

AW Server in Secured for RMF mode uses the AIDE integrity checker for checking the integrity of the filesystem, especially the EAT related files.

### NOTE

Following steps can be executed in Maintenance mode.

### 2.31.11.1 Checking integrity of the EAT related files

The integrity checking is done on a weekly basis, by running the `check_eat` script . This script checks the Audit Trail (EAT) and related config files integrity. If the check fails, the EAT logs file (`/var/log/audit.log`) is updated with specific lines containing “eat-integrity-failure” keys.

This script can also be run at any time to check the integrity. In a terminal execute the command:

```
/usr/local/share/hardening/tools/check_eat <Enter>
```

The result of the command is like:

```
Package eat changed unexpectedly
```

```
For details:
```

```
Run
```

```
aide -c /usr/local/share/hardening/stigs/APPSECDEV/common/aide.eat_conf.conf
```

As mentioned in the result of the command above, execute the below command to get details on the changes:

```
aide -c /usr/local/share/hardening/stigs/APPSECDEV/common/aide.eat_conf.conf
<Enter>
```

If the EAT configuration is changed in the Service Tools, to reset the integrity database, execute the below command in a terminal.

```
/usr/local/share/hardening/tools/finish_eat_conf_change <Enter>
```

### NOTE

It is the responsibility of the customer to ensure that the integrity is kept, by checking the EAT logs and, if integrity is broken, to fix it with the help of the GEHC FE.

### 2.31.11.2 Checking integrity of the file system

If the RMF mode is switched on, the AIDE check for the file system is implemented by a daily cronjob. This job is executed every day at 0:15.

The result is added to the rsyslog server, but similar to the EAT checking an error entry will appear in the `audit.log` (`/var/log/audit.log`).

The check can be executed manually with the following command:

```
aide -c /usr/local/share/hardening/stigs/APPSECDEV/common/aide.fs_conf.conf
```

# Chapter 3 Upgrade

## 3.1 Foreword

### NOTE

For the AW Server integrated within the CT/MR Console Environment (Edison HealthLink or CT Console), refer to [2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink on page 307](#) or [2.30 NanoCloud AW Server Installation in CT Console on page 373](#).

[Section 3.3 Quick Start Installation Guide - Software Upgrade on page 483](#)

This section gives an overview of the main steps to upgrade the software of an existing AW Server. When appropriate, it references the information detailed at chapter 2, for installation of a new AW Server. The steps described in this section for upgrading the software can also be used to simply reload the same software release.

### NOTICE

AW Server 3.1 / AW Server 3.2 release introduces the Ext. 4 filesystem that is faster than the Ext. 3 filesystem currently used by AW Server 2.0 and AW Server 3.0 releases.

When upgrading from AW Server 2.0 to the AW Server 3.2 release, you will have to make the following choice:

- The customer agrees that all images currently stored on AW Server are archived on another system (I.e: PACS) and that they can be erased from the AW Server.

It is therefore possible to upgrade the Image filesystem from Ext. 3 to Ext. 4.

The filesystem check (fsck) time will be faster than for AW Server 2.0 / AW Server 3.0 products.

- The customer DOES NOT agree that all images currently stored on AW Server can be deleted from the AW Server. It is therefore NOT possible to upgrade the Image filesystem from Ext. 3 to Ext. 4 and the filesystem will remain as Ext. 3. The filesystem check (fsck) time will be identical to what it was for AW Server 2.0 / AW Server 3.0 products, that is to say quite longer.

### NOTICE

EDS - Hardware upgrade for Seamless Integration:AW Server 2.0 / AW Server 3.0 upgrades to AW Server 3.2 Seamless Integration consist on a complete upgrade/swap to Virtual hardware. Only virtual hardware is supported with the AW Server 3.2 release / Seamless integration.

[Section 3.5 Entering the Maintenance Mode on page 486](#)

This section explains how to place the AW Server in Maintenance Mode before performing any maintenance operations.

[Section 3.6 Scalability Upgrade on page 488](#)

This section gives an overview of the main steps to:

- Add an AW Server in the cluster.
- Remove an AW Server from the cluster.
- Upgrade an AW Server 3.0 release cluster to AW Server 3.2 release.

- Upgrade the software to a more recent release within a AW Server 3.2 cluster.

### [Section 3.7 Hardware Upgrade on page 491](#)

This section gives an overview of the main steps to upgrade the hardware.

Currently, hardware upgrade consists on replacing the older hardware by a new hardware preloaded with OS and AWS Platform, or by a virtual AW Server (no preload).

### [Section 3.8 Applications Upgrade on page 491](#)

This section gives an overview of the steps to add new or to upgrade Applications.

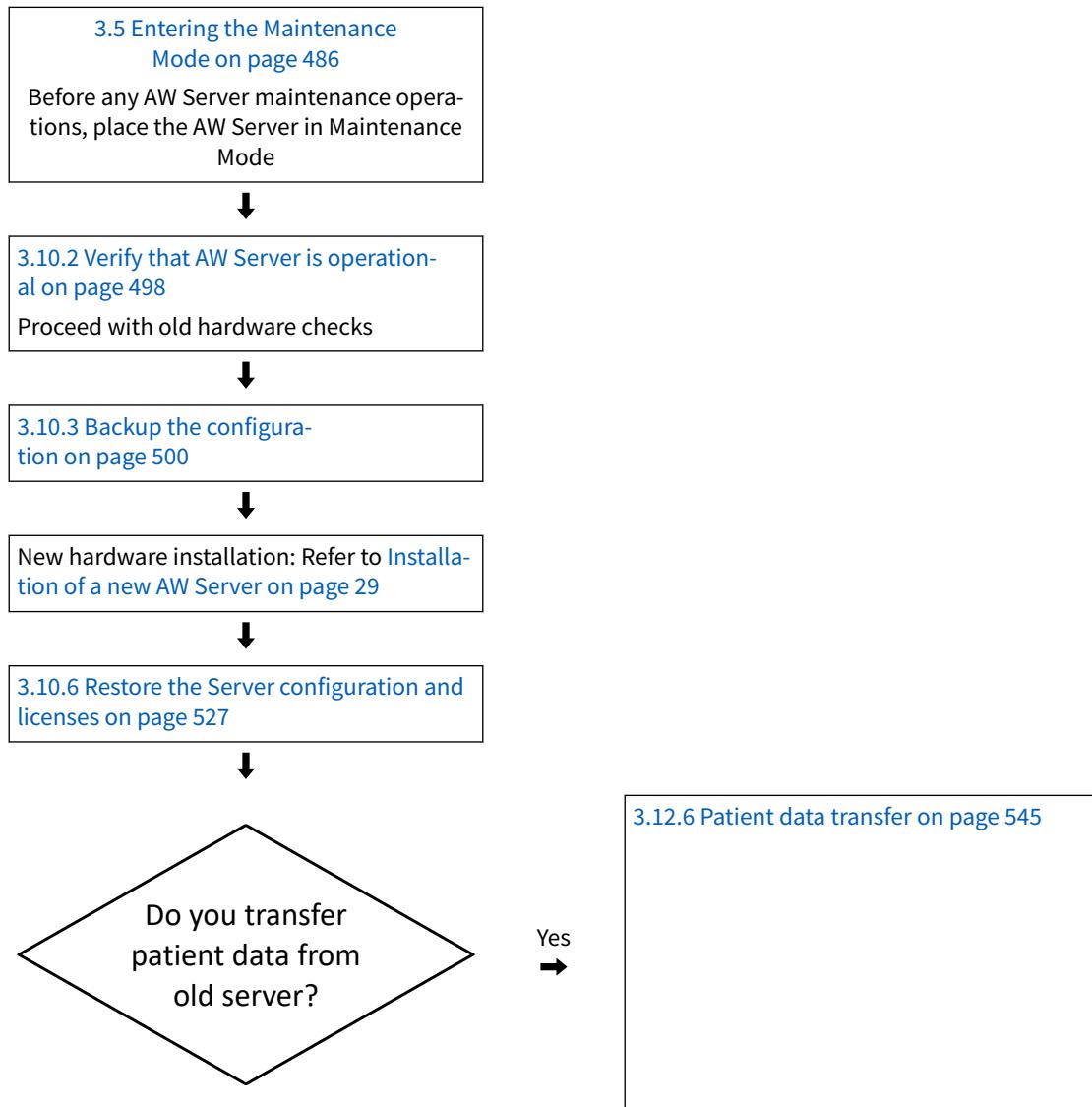
### [Section 3.9 System Configuration Restore Matrix on page 492](#)

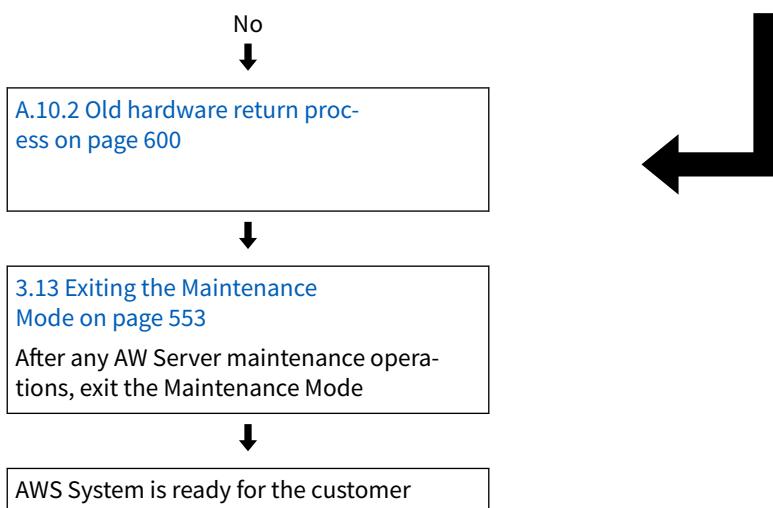
This section gives an overview of the System Configuration restoration rules.

#### **NOTICE**

When installing from electronic files, always refer to AW eDelivery Service Guide 5761599-8EN for detailed instructions.

## 3.2 Quick Start Installation Guide - Hardware Upgrade

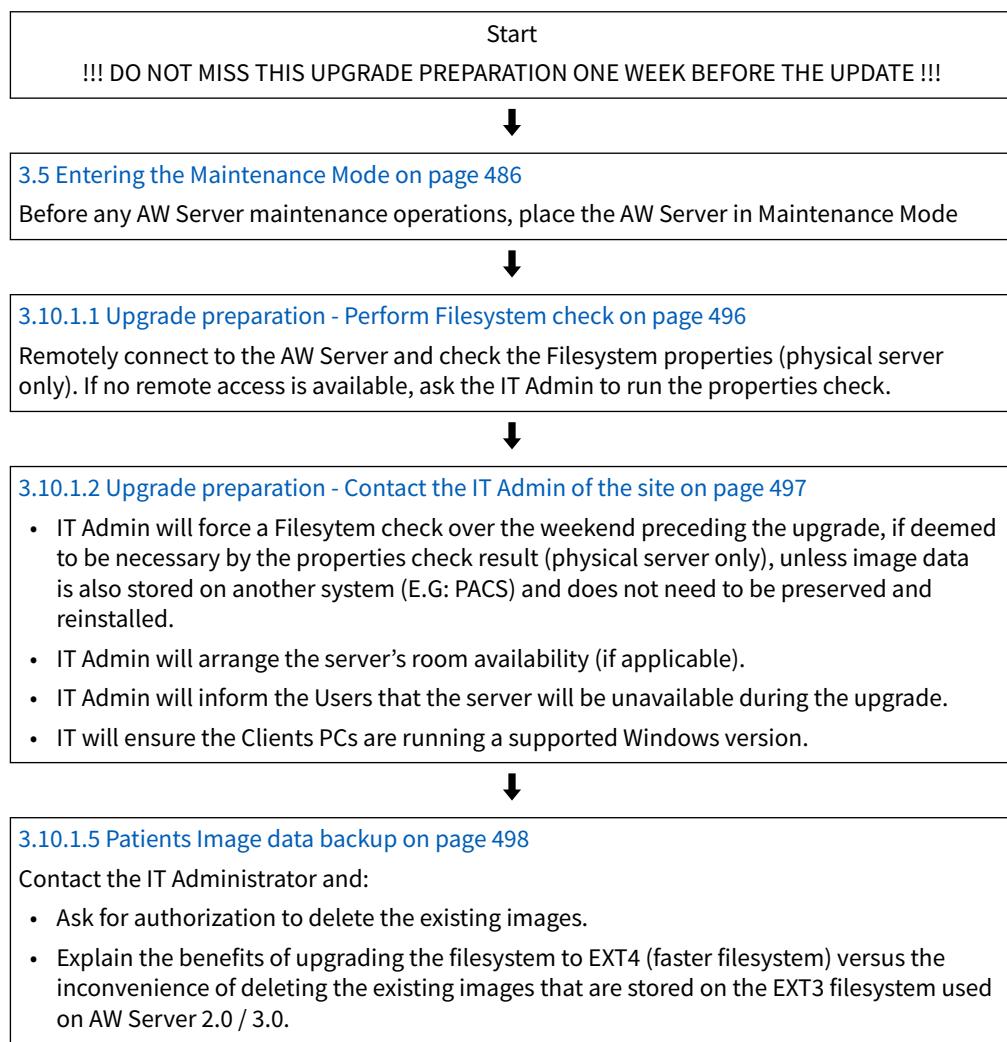




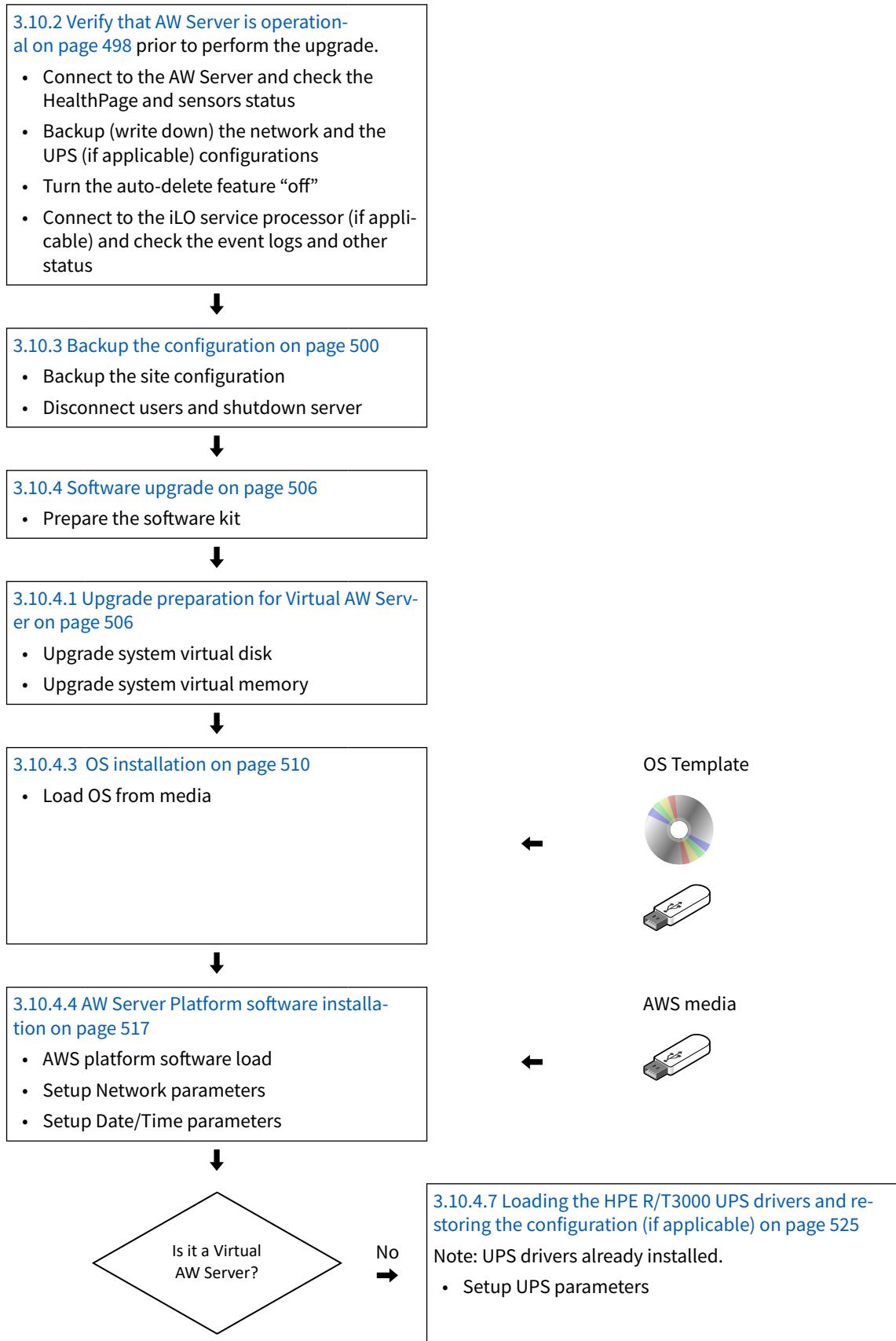
## 3.3 Quick Start Installation Guide - Software Upgrade

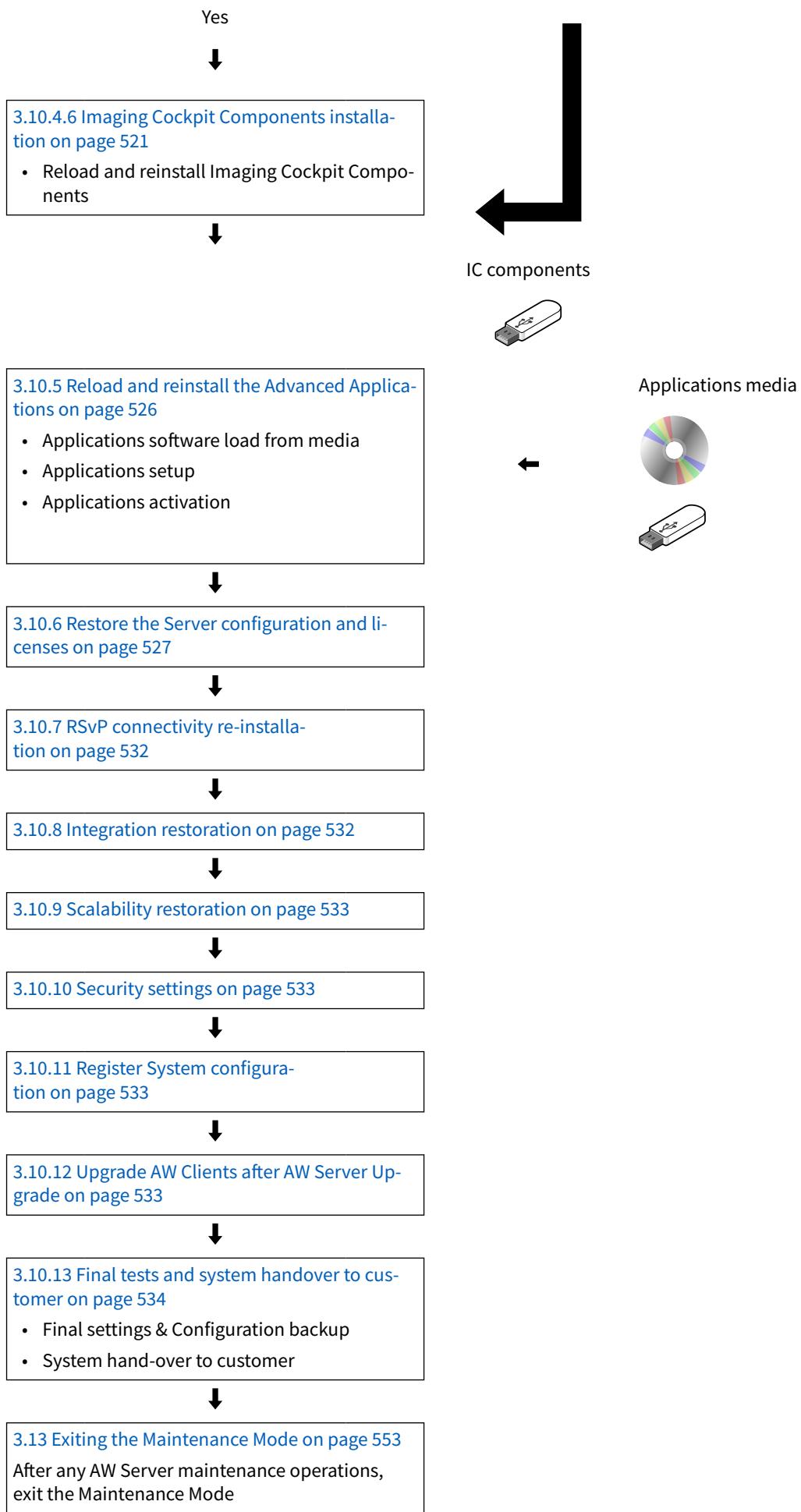
The following guide intends to summarize the installation steps to upgrade AW Server software. The upgrade instructions will be detailed along this manual in the different sections of [3.10 Job Card UPG001 - Software Upgrade](#) on page 495

Upgrade preparation, one week before the upgrade.



Proceeding to the upgrade.







AWS System is ready for the customer

## 3.4 Quick Start Installation Guide - Service Pack

The following guide intends to summarize the installation steps to install AW Server 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.

[3.5 Entering the Maintenance Mode on page 486](#)

Before any AW Server maintenance operations, place the AW Server in Maintenance Mode



[3.10.3 Backup the configuration on page 500](#)

Perform a full backup configuration.



[3.10.4.5 OS and AW Server Platform software](#)

Service Pack installation on page 518



[3.10.10.1 System Hardening on page 533](#)



[3.10.11 Register System configura-](#)

tion on page 533



[3.10.13 Final tests and system handover to cus-](#)

tomer on page 534

- Final settings & Configuration backup
- System hand-over to customer



[3.13 Exiting the Maintenance Mode on page 553](#)

After any AW Server maintenance operations, exit the Maintenance Mode

## 3.5 Entering the Maintenance Mode

The Maintenance Mode allows the AW Server to be "isolated" from the AW Server Clients in order to perform maintenance operations such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters...

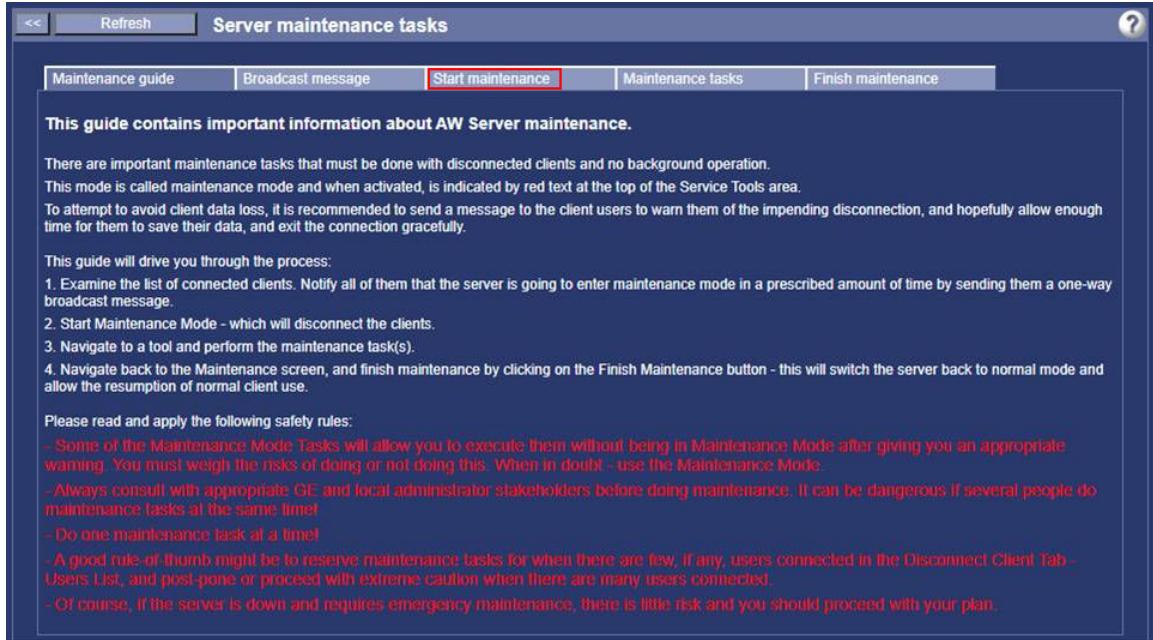
Before any such operations the AW Server shall be placed in Maintenance Mode.

**NOTE**

In Secured for RMF mode the procedure is the same on the UI, but please note that in the background AW Server will enable SSH and USB for the Maintenance period. When the user finishes the Maintenance on the Service Tools UI, AW Server in Secured for RMF mode will disable SSH and USB again.

Follow the below steps to place the AW Server in Maintenance Mode:

1. From the Client PC or the FE laptop open a web browser and connect to the AW Server IP address:  
`http://<AW server_IP_address>`
2. Launch Service Tools and login as **service**.
3. From the left menu, select **Maintenance > Maintenance** and select the **Start maintenance** tab.



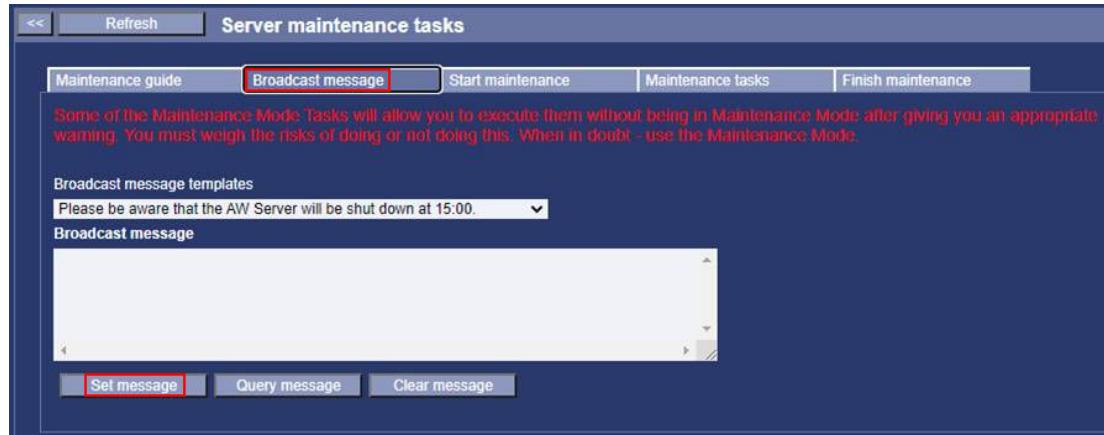
4. If users are connected, they appear as in the page:

User Name	User ID	User Roles	Client IP Address	Client Host Name
[redacted]	standard	[STANDARD]	10.77.65.65	192.168.0.6

Name	Session Start	Last Access
service	14-06-2021 11:02:38	14-06-2021 11:22:48
service	14-06-2021 14:08:26	14-06-2021 14:34:33

5. If users are connected, send a broadcast message to the users:

- Select the **Broadcast message** tab.



- Write a message or modify the default message to adapt it to your needs. An example of broadcast message could be: "AW Server will be shutdown in 5 minutes, save your work before exiting."
- Click on **Set message** to broadcast it.

#### NOTE

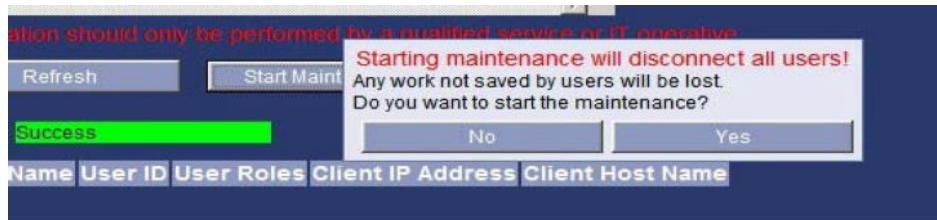
The **Query Message** button displays the last message entered. The **Clear Message** deletes all text in the message box. Always click **Clear Message** when done so that the last message is not inadvertently re-sent..

#### NOTICE

Allow a grace delay (a few minutes) for the users to save their work before disconnecting them by entering the Maintenance Mode.

- When the warning time has expired, come back to the **Start maintenance** tab and click on the **Start Maintenance** button to start the Maintenance Mode.

A pop-up confirmation message appears.



- Click on **Yes**.

Another pop-up states that you are in maintenance mode. And the Maintenance is in progress banner will display at the top of the Service Tools.



## 3.6 Scalability Upgrade

The following guide intends to summarize the installation steps for an AW Server Cluster upgrade, instructions that will be detailed all along this manual in the different sections of [3.11 Job Card UPG002 - Scalability Upgrade on page 535](#)

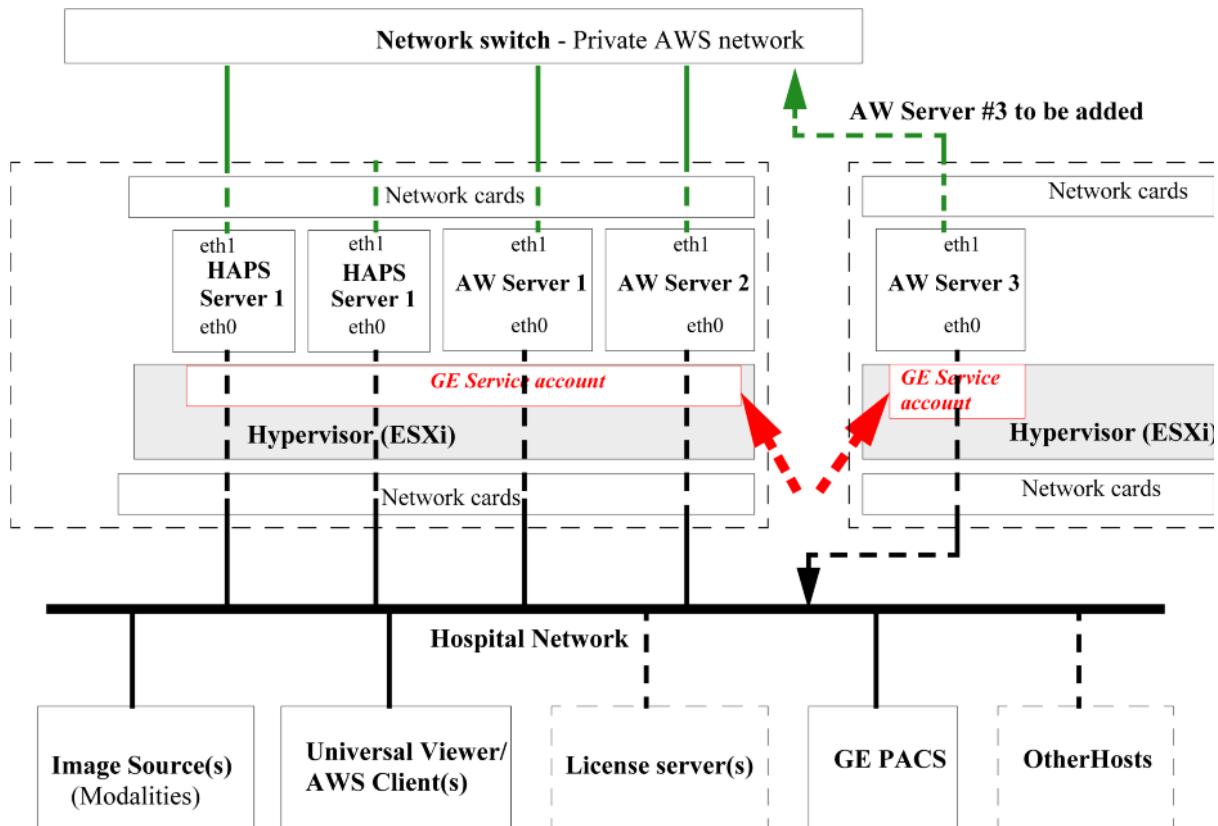
### 3.6.1 Adding an AW Server to an existing AW Servers Cluster

You have a cluster of AW Servers and you want to add a new AW Server to the cluster.

See [3.11.1 Adding an AW Server to an existing AW Servers Cluster on page 535](#).

#### NOTICE

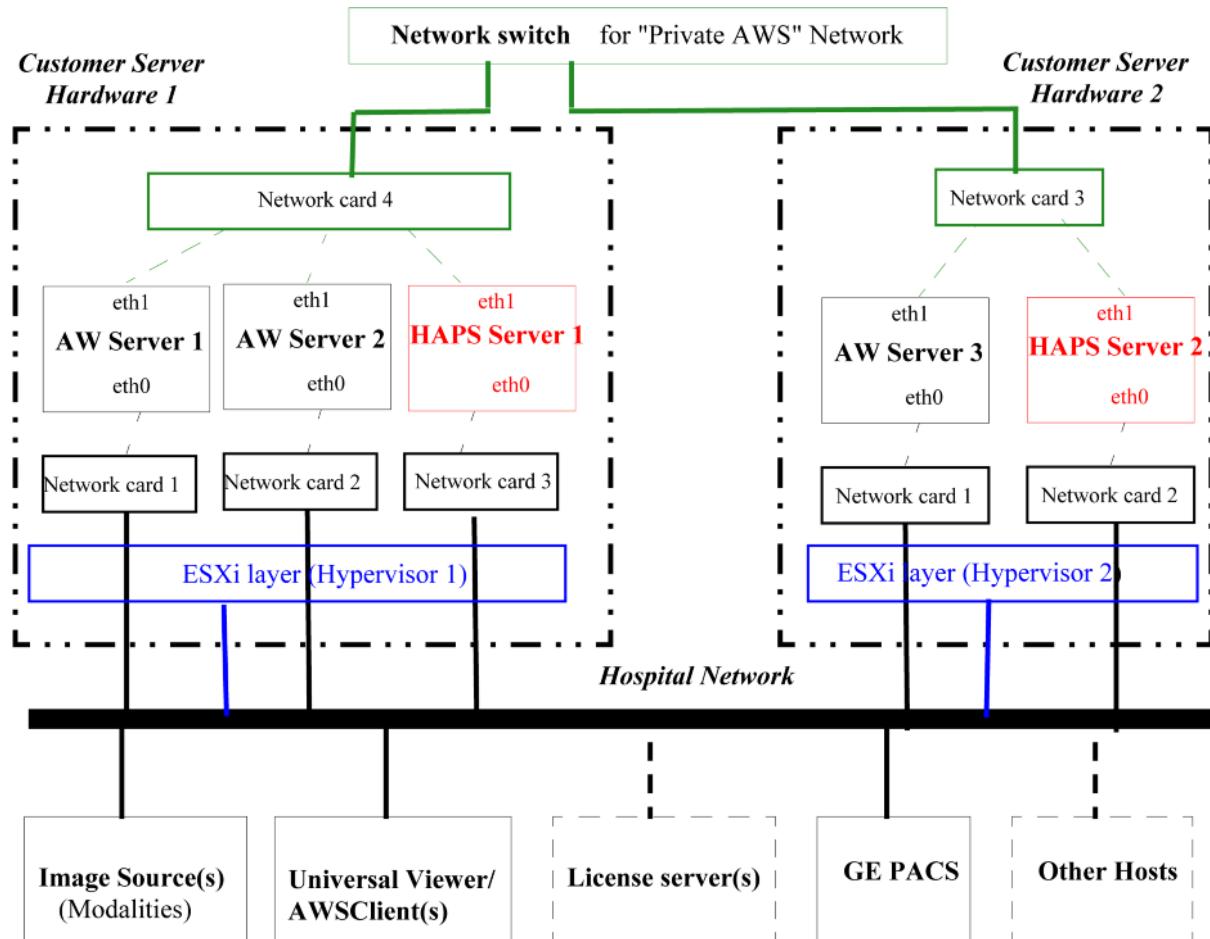
If the new virtual AW Server to be added to the cluster is NOT hosted on the same hypervisor, it is mandatory that the IT Admin also creates a similar GE Service account on the other hypervisor, so that the GE FE is able to "administrate" the new virtual AW Server.



#### NOTICE

In order to ensure proper hardware redundancy, it is strongly recommended that the two HAPS servers are hosted on different Hypervisor hardware (see after).

***Example of a cluster of 3 virtual AW Servers hosted on two different servers hardware***



### 3.6.2 Removing an AW Server from an AW Servers Cluster

You have a cluster of AW Servers and you want to remove an AW Server from the cluster.

See [3.11.2 Removing an AW Server from an AW Servers Cluster on page 536](#)

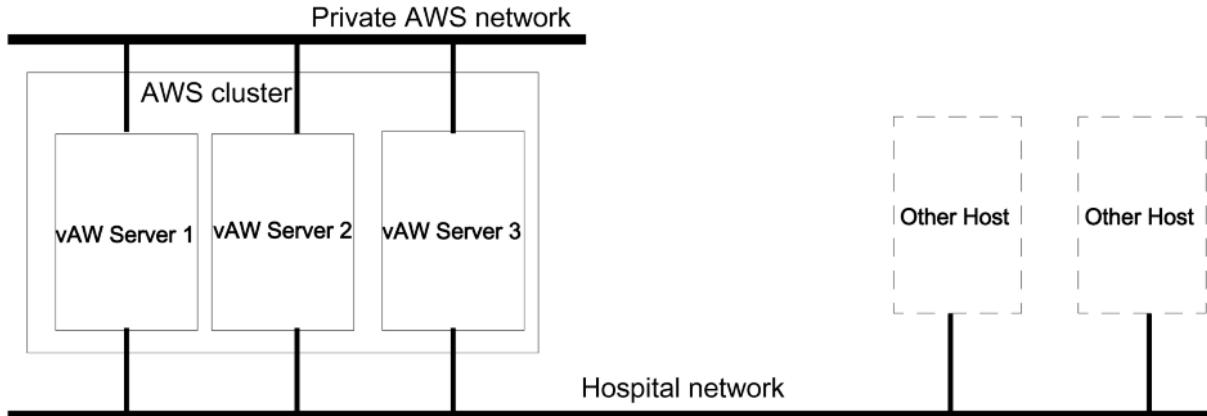
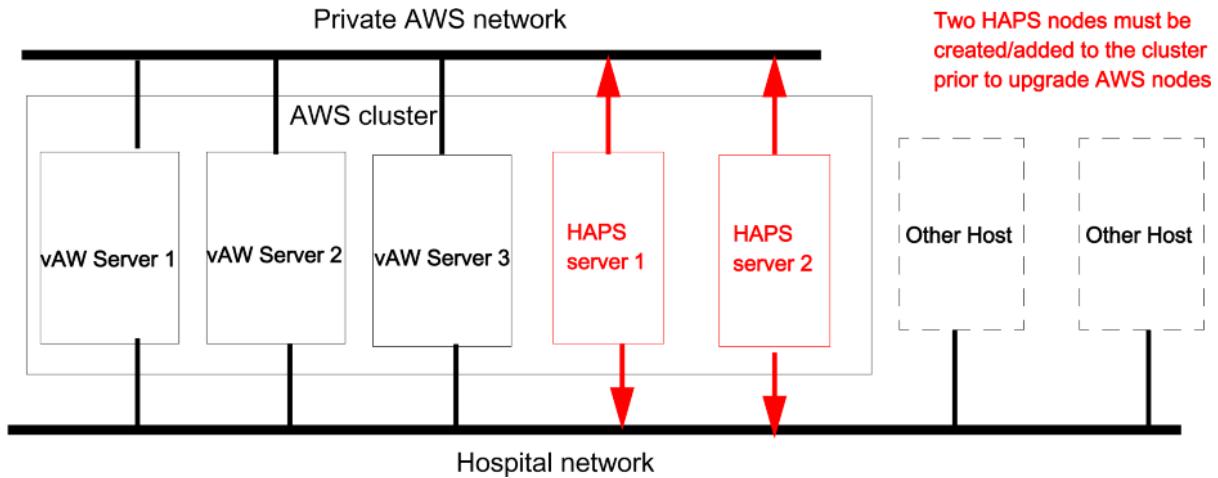
### 3.6.3 Upgrading an AW Server 3.0 Cluster to AW Server 3.2 release

You have a cluster of AW Server 3.0 and you want to upgrade the servers to **AW Server 3.2** release.

See [3.11.3 Software Upgrade within a Cluster on page 537](#)

#### NOTICE

**AW Server 3.2** release introduces the Preferences Sharing servers for Scalability. Two HAPS (High availability Preferences Sharing) servers must be created and added to the cluster.

**Figure 3-1 AW Server 3.0 cluster example - before upgrade****Figure 3-2 AW Server 3.0 cluster example - during upgrade**

### 3.6.4 Software Upgrade within an AW Servers Cluster

You have a cluster of **AW Server 3.2** and you want to upgrade to a more recent release, the software of the AW Servers and/or Applications.

See [3.11 Job Card UPG002 - Scalability Upgrade on page 535](#) - [3.11.3 Software Upgrade within a Cluster on page 537](#)

## 3.7 Hardware Upgrade

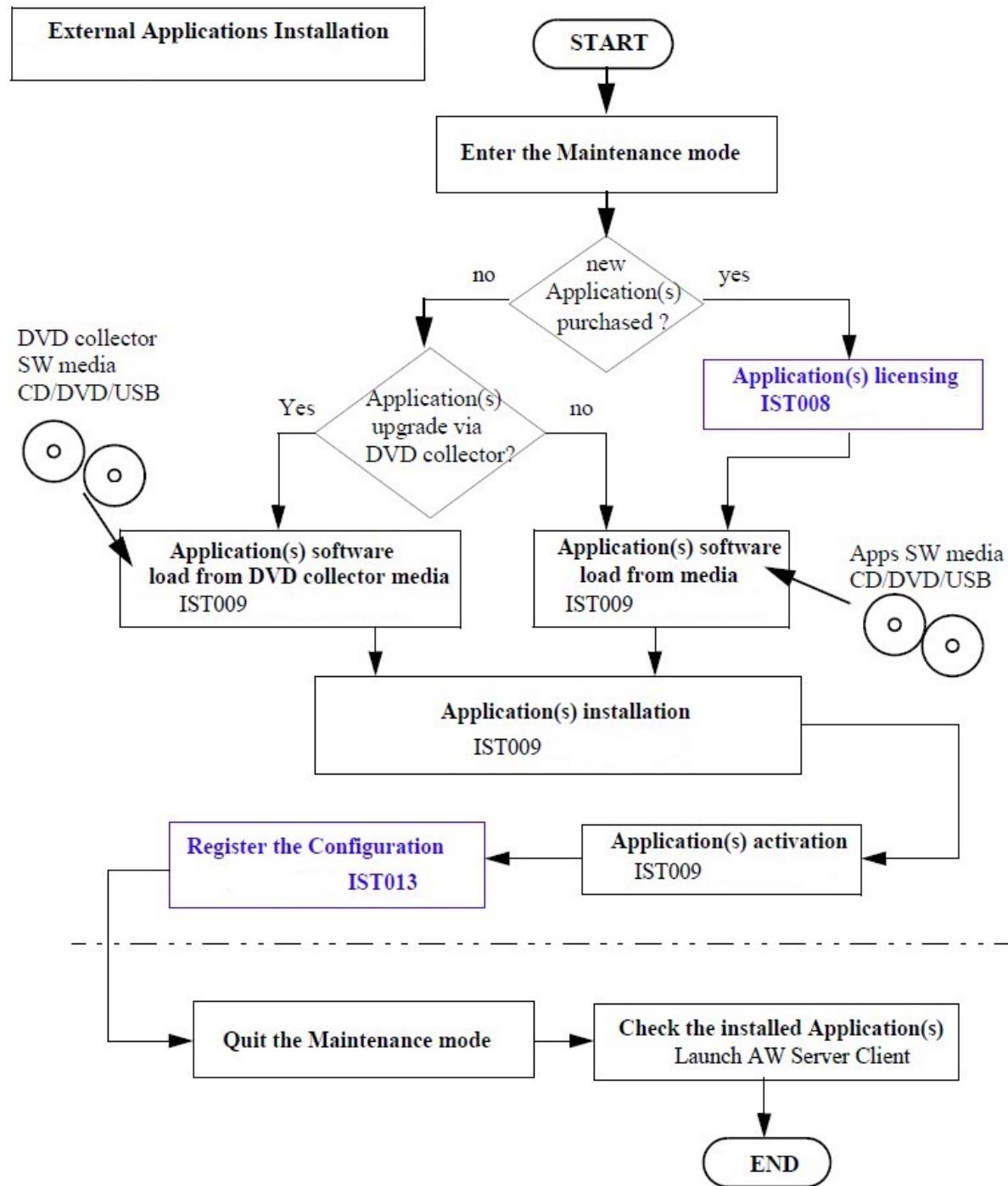
You have an older AW Server hardware that shall be upgraded.

Currently, hardware upgrades consist of a complete hardware replacement.

See [3.12 Job Card UPG003 - Hardware Upgrade on page 543](#)

## 3.8 Applications Upgrade

You have Applications that shall be upgraded, or the site has purchased new Applications.



## 3.9 System Configuration Restore Matrix

Prior to software reload or hardware swap, the System configuration should be saved.

(See [3.10.3 Backup the configuration on page 500](#))

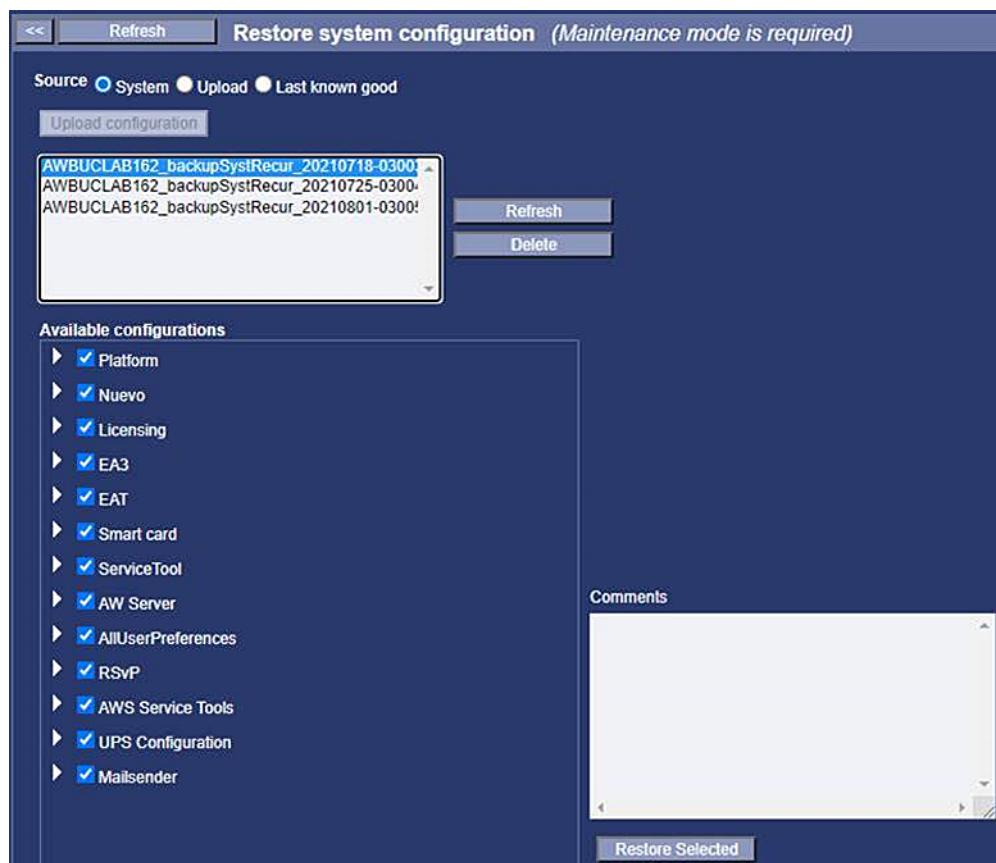
Upon software reload or hardware swap, the System configuration or part of it can be restored.

(See [3.10.6 Restore the Server configuration and licenses on page 527](#))

The System configuration Restore matrix below addresses the following cases:

1. AW Server 3.2 to AW Server 3.2 software re-installation or upgrade.
  - a. All parameters are automatically restored **except for passwords**.
2. AW Server 3.1 to AW Server 3.2 software re-installation or upgrade.

- a. Items marked **OK** are automatically restored.
  - b. Items marked **To be unchecked** have to be unchecked in the restore sys config menu
3. **AW Server 2.0/ AW Server 3.0** to AW Server 3.2 software upgrade.
- a. Items marked **OK** are automatically restored.
  - b. Items marked **Not restored** have to be configured manually.
4. **Hardware** upgrade to new **hardware** or to **Virtual** hardware.
- a. Items marked **OK** are automatically restored.
  - b. Items marked **Not restored** have to be configured manually.
  - c. Items marked **To be unchecked** have to be unchecked in the restore sys config menu.



### Restoration matrix

Legend	Automatically restored - No action needed
	Not automatically restored - Configuration needed
	Not applicable
	To be unchecked in restore menu before restoring.

ITEM	SUB-ITEM	AWS3.2 to AWS3.2 SW rein-stall	AWS3.1 to AWS3.2 SW upgrade	AWS2.0/3.0 SW upgrade to AWS3.2	HW upgrade to AWS3.2 new HW / VM
<b>Platform</b>	/etc/cups	OK	N/A	N/A	N/A
	/etc/ntp.conf	OK	OK	OK	OK
	/var/lib/ServiceTools_AWS/conf platform-Config.xml	OK	OK	not restored	not restored

	/export/home/sdc/icm/resources/config.icmregkey	OK	OK	not restored	not restored
<b>Nuevo</b>	/export/home/sdc/nuevo/resources/network/network-cfg.xml	OK	OK	OK	OK
	/export/home/sdc/nuevo/resources/browser/sessions.properties	OK	OK	OK	OK
	/export/home/sdc/nuevo/resources/printManager/printer-cfg.xml	OK	OK	OK	OK
	/export/home/sdc/nuevo/resources/system/auto_delete_preference.properties	OK	OK	OK	OK
<b>Licensing</b>	/usr/share/CoLA/Cola_config.txt	OK	OK	OK	OK
	/usr/share/CoLA/GemsLicense	OK	OK	OK	not restored
	/usr/share/FL_Server/GemsLicense	OK	OK	OK	not restored
	/var/lib/ServiceTools_AWS/install/install/activatedLicenses.txt	OK	OK	not restored	not restored
<b>EA3</b>	/usr/share/gehc_security/ea3/configs/	OK	OK	OK	OK
	/usr/share/gehc_security/ea3/userdb/	OK	OK	OK	OK
<b>EAT</b>	/usr/share/gehc_security/eat/configs/	OK	OK	OK	OK
<b>Smart Card</b>	/var/lib/ServiceTools/conf/smartCardAuth.properties	OK	N/A	N/A	N/A
	/etc/pki/tls/certs/client_cas	OK	N/A	N/A	N/A
<b>ServiceTool</b>	/var/lib/ServiceTools/conf/contact-list.xml	OK	OK	OK	OK
	/var/lib/ServiceTools/conf/device-cfg.xml	OK	OK	OK	to be unchecked
	/var/lib/ServiceTools/conf/GIB.xml	OK	OK	OK	to be unchecked
	/var/lib/ServiceTools/conf/cmd-logging.properties	OK	OK	N/A	N/A
	/var/lib/ServiceTools/conf/rmiserver-logging.properties	OK	OK	N/A	N/A

ITEM	SUB-ITEM	AWS3.2 to AWS3.2 SW rein-stall	AWS3.1 to AWS3.2 SW upgrade	AWS2.0/3.0 SW upgrade to AWS3.2	HW upgrade to AWS3.2 new HW / VM
	/var/lib/tomcat6/webapps/Service-Tools/WEB-INF/classes/logging.properties	OK	OK	N/A	N/A
	/var/lib/ServiceTools/conf/SNMPConfig.xml	OK	OK	OK	OK
	/var/lib/ServiceTools/conf/stlanguage.xml	OK	OK	OK	OK
	/var/lib/ServiceTools/conf/backup-recur-list.xml	OK	N/A	N/A	N/A
	/tmp/recurrent_backup	OK	OK	not restored	OK
<b>AW Server</b>	/export/home/sdc/UserPrefs/	OK	OK	OK	OK
	/export/home/sdc/Prefs/	OK	OK	OK	OK
	/export/home/sdc/server/prefs/	OK	OK	OK	OK
<b>RichClientUserPreferences</b>	/export/home/sdc/users/	OK	OK	OK	OK

	/export/home/sdc/client/prefs/	OK	OK	OK	OK
<b>RSvP</b>	/tmp/rsvpagent.tar.gz	OK (restore allowed for the same System ID (CRM Number))	N/A	N/A	N/A
<b>Software Download</b>	/export/home/sdc/Prefs/swd/	OK	OK	OK	OK
<b>AWS Service Tools</b>	/var/lib/ServiceTools_AWS/conf/cmd-logging.properties	OK	OK	N/A	OK
	/var/lib/ServiceTools_AWS/conf/rmiserver_aws-logging.properties	OK	OK	N/A	OK
	/var/lib/tomcat6/webapps/ServiceTools_AWS/WEB-INF/classes/logging.properties	OK	OK	N/A	OK
	/var/lib/ServiceTools_AWS/conf/PreprocessingConf.xml	OK	OK	OK	OK
	/var/lib/ServiceTools_AWS/conf/PACSConfig.xml	OK	OK	OK	OK
<b>UPS Config</b>	/tmp/upsconfig	OK	OK	OK	OK

## 3.10 Job Card UPG001 - Software Upgrade

### Manpower requirement:

One Field Engineer for 5 hours. This time includes the upgrade of one client only.

If the Customer requests additional Clients to be upgraded by GE then FE will bill the GE FMI account.

This may require additional scheduling and coordination.

### NOTICE

The SUN X4450 hardware based AW Server is not supported with AW Server 3.2 release.

### Summary of tasks

The GEHC Field Engineer is responsible for the following:

- Section [3.10.1 Upgrade Preparation - One week before the upgrade on page 496](#): Prior to go to the site - !!! DO NOT MISS THIS STEP !!!
  - Contact IT administrator - Remotely connect to the site and launch the Filesystem Check.
  - Contact the IT administrator of the site for any change needed to the current implementation
- Section [3.10.2 Verify that AW Server is operational on page 498](#):
  - Verify that the AW Server is fully operational before proceeding to the reload/upgrade
- Section [3.10.3 Backup the configuration on page 500](#):
  - Save the network configuration
  - Save the UPS (if applicable to your site) configuration
  - Properly disconnect any connected Users prior to do the upgrade

- Backup of the site configuration prior to do the upgrade
- Section [3.10.4 Software upgrade on page 506](#):
  - Load the Linux Operating system (Load From Cold)
  - Load the AW Server platform software (Load From Cold)
    - Configure Network and Time zone
  - Reinstall the UPS drivers and configure (if applicable)
- Section [3.10.5 Reload and reinstall the Advanced Applications on page 526](#)
- Section [3.10.6 Restore the Server configuration and licenses on page 527](#)
- Section [3.10.7 RSvP connectivity re-installation on page 532](#) `Restore / reinstall RSvP connectivity`
- Section [3.10.8 Integration restoration on page 532](#) `Restore / reinstall Integration (if applicable)`
- Section [3.10.9 Scalability restoration on page 533](#) (if applicable).
- Section [3.10.10.2 Passwords restoration on page 533](#)
- Section [3.10.11 Register System configuration on page 533](#)
- Section [3.10.12 Upgrade AW Clients after AW Server Upgrade on page 533](#)
- Section [3.10.13 Final tests and system handover to customer on page 534](#)

## 3.10.1 Upgrade Preparation - One week before the upgrade

### 3.10.1.1 Upgrade preparation - Perform Filesystem check

#### NOTICE

#### DO NOT MISS THIS STEP

About one week before going to the site, the system must be rebooted and Filesystem check must be performed. Worst case scenario could be 8 hours for a Filesystem check for a full database.

**We recommend scheduling it overnight, starting Friday evening for example.**

Note that very long Filesystem check time is not applicable for Full or Seamless integration - The main Image database is on the PACS - Only a reduced image database remains on the AW Server for reconstructed images, so the AW Server unavailability during FSCK time is not significant.

1. Launch the Service Tools.
2. Login as `service`.
3. If the AW Server is not in Maintenance Mode, proceed to [3.5 Entering the Maintenance Mode on page 486](#).
4. Click on **Tools** then **Terminal** in the sub menu.
5. Click on **Connect** button to open a Terminal window.
6. Login as `root`.
7. Reboot the server forcing the filesystem check.

```
touch /forcefsck <Enter><Enter>
```

```
reboot <Enter>
```

Filesystem check can take several hours depending on the number of images stored on the system. You can monitor the progress on the terminal (KVM) in the server room or with the console redirection of the iLO. When Welcome to Scientific Linux screen displays, press the **<Esc>** key to view the progress message.

```
Starting udev: [ OK ]
Setting hostname awsvc03: [ OK ]
Setting up Logical Volume Management: No volume groups found [ OK ]
Checking filesystems
/dev/sdb3: clean, 146743/3276800 files, 3179742/13107200 blocks
/dev/sda1 has gone 201 days without being checked, check forced.
/dev/sda1: 18/244320 files (0.0% non-contiguous), 33647/976128 blocks
/dev/sda2 has gone 201 days without being checked, check forced.
/dev/sda2: ===== \ 96.1%
```

#### **NOTICE**

**Do not interrupt the fsck (filesystem check) process. Risk of data loss.**

### **3.10.1.2 Upgrade preparation - Contact the IT Admin of the site**

Prior to going on site to perform the FMI tasks, you should ensure proper training as well as contact the site IT administrator so that they can make the necessary arrangements:

- **IT Admin should inform all users** of the scheduled FMI date, and that.
  - The AW Server will be unavailable for several hours during the upgrade.
  - DICOM image transfer from modalities to the AW Server will not be possible during the upgrade.
- **IT Admin should ensure that all Client PC's** (needing to be upgraded to the AW Server 3.2 release or any new PCs to be used) are running the appropriate Windows supported version. Refer to AW Server 3.2 login page for supported OS's.
- **IT Admin should arrange access to the Server Room if applicable.**
- **IT Admin should confirm if configuration changes** are needed (i.e: IP address change, Default gateway, etc ...)
- **IT Admin should confirm that all image data stored** on the AW Server are also stored on other DICOM hosts such as PACS, in case of damage to the database.
- **IT Admin should be prepared to upgrade all clients** upon completion of the FMI. The IT Admin should be aware that the FE will upgrade and validate the AWS Client software only on one Client PC.

### **3.10.1.3 Floating License Server**

#### **NOTICE**

If AW Server is acting as a Floating License Server for AW Workstations as well, then the users will lose access to their floating applications during this time. Please plan the upgrade while considering the impact on all AW standalone Users, not just AW Server users.

### **3.10.1.4 Software Changes**

The AW Server software may change from the time of this writing. If there is a discrepancy between this document and the screens you see, use your best judgment to complete this procedure as it was originally intended.

### 3.10.1.5 Patients Image data backup

Patient Images data can be preserved during software reload and be reinstalled when software load is complete.

#### NOTICE

**However**, for AW Server 2.0 / AW Server 3.0 upgrade to AW Server 3.2, **we strongly recommend to proceed to Ext3 to Ext4 filesystem upgrade** in order to benefit of a faster filesystem, but consequently, you will have to accept that the image data shall be deleted. In this case, make sure to get customer agreement prior to proceed to image deletion.

#### NOTE

Unless your AW Server 3.1 system is an upgrade from AW Server 2.0 release that was done without image deletion, it is already running Ext4 filesystem, so images from AW Server 3.1 can be preserved during upgrade to AW Server 3.2

#### NOTICE

Make sure that your customer has properly saved the patients image data on another system (PACS, DVDs) prior to perform the software upgrade.

## 3.10.2 Verify that AW Server is operational

Verify that the AW Server is operational prior to proceed with the software upgrade.

Sections [3.10.2.1 Check the hardware indicator LEDs \(hardware server only\) on page 498](#) and [3.10.2.2 Check the iLO Service processor \(hardware server only\) on page 498](#) are not applicable to virtual AW Servers.

### 3.10.2.1 Check the hardware indicator LEDs (hardware server only)

#### These actions shall be performed in the Server room

- Make sure that no errors are reported, both on the server and the disks array (if applicable).
- Check for any yellow LED that would report an error condition.
- Make sure the keyboard, mouse and monitor are connected and operational.
- At the keyboard, login as **root**.
- Check that the system responds to command lines

**df -k <Enter>**

### 3.10.2.2 Check the iLO Service processor (hardware server only)

#### These actions shall be performed on the Client PC or FE laptop

- Connect to the HP iLO Service processor
  - [http://<iLO\\_IP\\_address>](http://<iLO_IP_address>)
  - Login as **root**.

#### NOTICE

If hardware errors are reported by the system, they should be fixed prior to upgrading the software.

**Figure 3-3 Example with the iLO 5 Service Processor (it is similar for iLO 4 and iLO 3)**

The screenshot shows the iLO 5 Service Processor interface. On the left is a sidebar with various navigation options: 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, Security, Management, and Intelligent Provisioning. The main area is titled "System Information - Health Summary". Below it is a tab bar with "Summary" (selected), Processors, Memory, Network, Device Inventory, and Storage. The main content area is titled "Subsystems and Devices" and contains a table of system components and their status:

Subsystems and Devices	Status
Agentless Management Service	ⓘ Not available
BIOS/Hardware Health	✅ OK
Fan Redundancy	✅ Redundant
Fans	✅ OK
Memory	✅ OK
Network	✅ OK
Power	⚠️ Not Redundant
Power Supplies	❌ Failed
Processors	✅ OK
Smart Storage Energy Pack	✅ OK
Storage	✅ OK
Temperatures	✅ OK

- Click on **System Information** tab, and navigate through the Fans, Temperatures, Memory... to make sure no error conditions are flagged.

### 3.10.2.3 Connect to the AW server

**These actions shall be performed on the Client PC or FE laptop**

- Open an Internet Navigator
- Connect to the AW Server IP address  
**http://<AW server\_IP\_address>**
- Login as **service**.

#### 3.10.2.3.1 Check the HealthPage

The Healthpage is displayed. Check that no errors are reported in the Healthpage.

Any reported issue should be investigated prior to do the upgrade.

Refer to the AWS Service Manual.

The image compares two HealthPage examples. On the left is the "HP hardware AW server example" and on the right is the "Virtual AW Server example". Both pages show a table of system components and their status. The HP hardware page includes a "Sensor Details" button, while the Virtual AW Server page includes a "Status details" button.

Hardware Subsystem	Status
Temperature	OK
Fan Status	OK
Voltage	Not applicable
Power Status	OK
UPS Status	Not applicable
RAID Status	OK

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

### 3.10.2.3.2 Turn auto-delete feature OFF

#### NOTICE

The auto-delete feature may not have the exact same low mark and high mark limits between the Gen2 and Gen3 releases. To avoid the risk of unintentionally deleting images, turn the auto-delete OFF prior to proceed with the upgrade.

- AW Server 1.0: No upgrades from Gen 1 are supported for AW Server 3.2
- AW Server 2.0 and AW Server 3.x:
  - The Auto-delete feature can be turned off directly from the Service Tools / **Initial Configuration** menu.

### 3.10.2.3.3 Verify Preferences ownership

Verify the Preferences ownership before performing the AW Server shutdown.

At the FE Laptop or Client PC that is connected by the network to the AW Server.

- Open a **Terminal** from the Service Tools / **Tools** (or **Utilities** - AW Server 2.0) menu.
- Log as **root** (if not already done).
- Type:

**cd /export/home/sdc <Enter>** (AW Server 2.0)  
OR

**cd /var/prefs <Enter>**  
**ls -al users <Enter>**

If Preferences do NOT belong to sdc users and sdc group, type the following command line:

**chown -R sdc:sdc users <Enter>**

### 3.10.2.4 Important information about Hostnames

If the hostname has been properly chosen for the previous AW Server release, you should not have to change it for the upgrade, and we recommend that you keep the same.

For hostname characters limitations, refer to [A.2 Specific field - Characters rules and limitations on page 555](#).

#### NOTE

Due to a policy change at the new OS (Redhat 7) it is not allowed anymore to have an underscore (“\_”) nor capital letters [A-Z] in the hostname. So, it means that if the hostname of the AW Server being upgraded contains an underscore (“\_”), it should be removed or replaced by authorized character (e.g.: hostname changes from **AWS\_name** to **awsname** or **aws-name**).

In this case, this will impact the systems/devices using this AW Server as a DICOM Remote Node. They will have to change the hostname as well as the AE Title (as it is the same as the hostname) manually on these systems/devices.

### 3.10.3 Backup the configuration

### 3.10.3.1 Backup the Network configuration

#### NOTICE

The System configuration backup utility from AW Server Service Tools does not include the Network parameters. You must SAVE THE NETWORK SETTINGS CONFIGURATION BY WRITING DOWN THE DATA FOR ONGOING USE. THE NETWORK CONFIGURATION MUST ALWAYS BE CONFIGURED AFTER AN OS SOFTWARE LOAD AND IS NOT SAVED BY THE AW SERVER SERVICE TOOLS BACKUP.

#### NOTE

In case of Full, Seamless or DICOM Direct Connect Integration (configuration without Image Database partition), all the backups shall be done on another system (PACS, Client PC, etc.), as there is no built-in "backup" partition on the AW Server.

Before performing the site configuration backup, you must write down: Hostname, IP address, and AE Title from AW Server HealthPage screen – and also the *Network Prefix* by running **ip addr show eth0** command line from a terminal window, and the Default Routers by running **ip route** command line.

#### From a network connected PC or laptop

1. Display the AW Server HealthPage.
2. Login to Service Tools as **service**.
3. **From AW the Server HealthPage:**
  - a. Write down: Hostname, IP address and AE Title.
    - Hostname : \_\_\_\_\_
    - IP address : \_\_\_\_\_
    - AE Title: \_\_\_\_\_

**Figure 3-4 Example of AW Server HealthPage**

<b>System Configuration</b>	
System ID (CRM Number)	AWBUCUCLAB243
Platform version	aws-3.2-4.2-2129.2-c8bbb739
Hostname / IP Address	bucaw70-243 / eth0: 3.249.70.243
Encrypted (TLS) AET / Port	bucaw70-243 / 2762
Plain AET / Port	bucaw70-243 / 4006
CPU (8)	Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9

- b. Open a Terminal from the Service Tools / Tools menu, login as **root**.
  - To display the Network prefix
    - i. type:  
**ip addr show eth0 <Enter>**
    - ii. Write down the Network Prefix value (Network Prefix is 23 in example below).
      - Network Prefix: \_\_\_\_\_

**Figure 3-5 Example of ip screen**

```
[root@bucaw70-241 ~]# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:8a:a8:a7 brd ff:ff:ff:ff:ff:ff
        inet 3.249.70.241/23 brd 3.249.71.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fea:a8a7/64 scope link
            valid_lft forever preferred_lft forever
[root@bucaw70-241 ~]#
```

- To display the Default Gateway:

- i. type:

**ip route <Enter>**

- ii. Write down the Default Gateway value (Gateway is 3.249.15.254 in example below).

- Default Gateway:\_\_\_\_\_

**Figure 3-6 Example of route screen**

```
[root@bucaw70-241 ~]# ip route
default via 3.249.71.250 dev eth0 proto static metric 100
3.249.70.0/23 dev eth0 proto kernel scope link src 3.249.70.241 metric 100
[root@bucaw70-241 ~]#
```

- To display the DNS servers (if any):

- i. type:

**cat /etc/resolv.conf <Enter>**

- ii. Write down the DNS server(s) value (2 servers in example below).

- DNS servers :\_\_\_\_\_
- Domain names :\_\_\_\_\_

**Figure 3-7 Example of resolv.conf screen**

```
[root@bucaw70-241 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 10.220.220.220
nameserver 10.220.220.221
[root@bucaw70-241 ~]#
```

The Hostname, IP Address, AE Title (DNS Hostname) and Netmask/Network Prefix will be used later during the software installation process.

Alternatively, all this information can be obtained from the IT department of the hospital.

### 3.10.3.2 Backup the UPS configuration

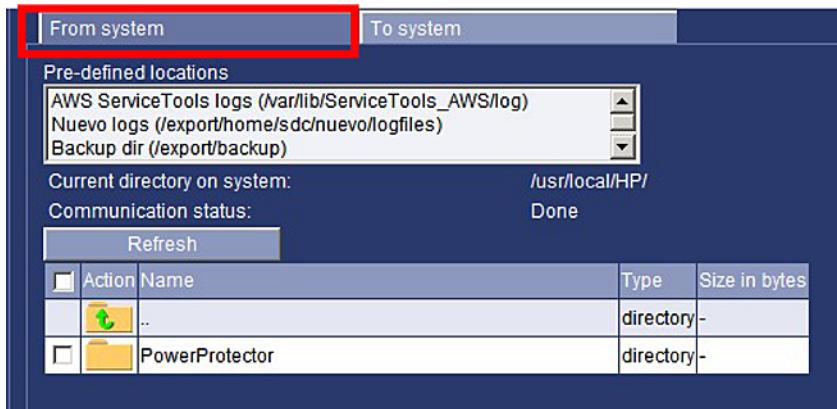
The System configuration backup utility from AW Server Service Tools does not include the UPS parameters. If applicable to your site, backup the UPS configuration.

#### 3.10.3.2.1 Backup the HP UPS setup

- Stop the HPPP service:

**systemctl stop HP-HPPP <Enter>**

- Connect to the Service Tools as **service**.
- Launch the **File Transfer** utility from the **Tools** menu.
- Select **From system** tab:



- Scroll down and click to move to **usr** directory, then click to move to **local** directory, then to **HP** directory, then to **PowerProtector** directory.
- Move to **configs** directory and transfer the configuration files to the Client PC or FE laptop, by clicking on **Pull from system** button.
- Acknowledge the popup message mentioning the file size to be transferred, and choose the location on your PC where to save the file.
- When done, move back to **PowerProtector**, then move to **db** directory and transfer the configuration files to the Client PC or FE laptop.
- Restart the HPPP service:

**systemctl start HP-HPPP <Enter>**

### 3.10.3.3 Backup the Site configuration

The AW Server is placed in Maintenance Mode. If not refer to [3.5 Entering the Maintenance Mode on page 486](#).

In this section, we backup the site configuration and shutdown the AW server.

#### NOTE

The System configuration backup also embeds backup of the User Preferences.

First, make sure you are still logged as **service** (see section [3.10.2.3 Connect to the AW server on page 499](#)).

#### Backup the system configuration:

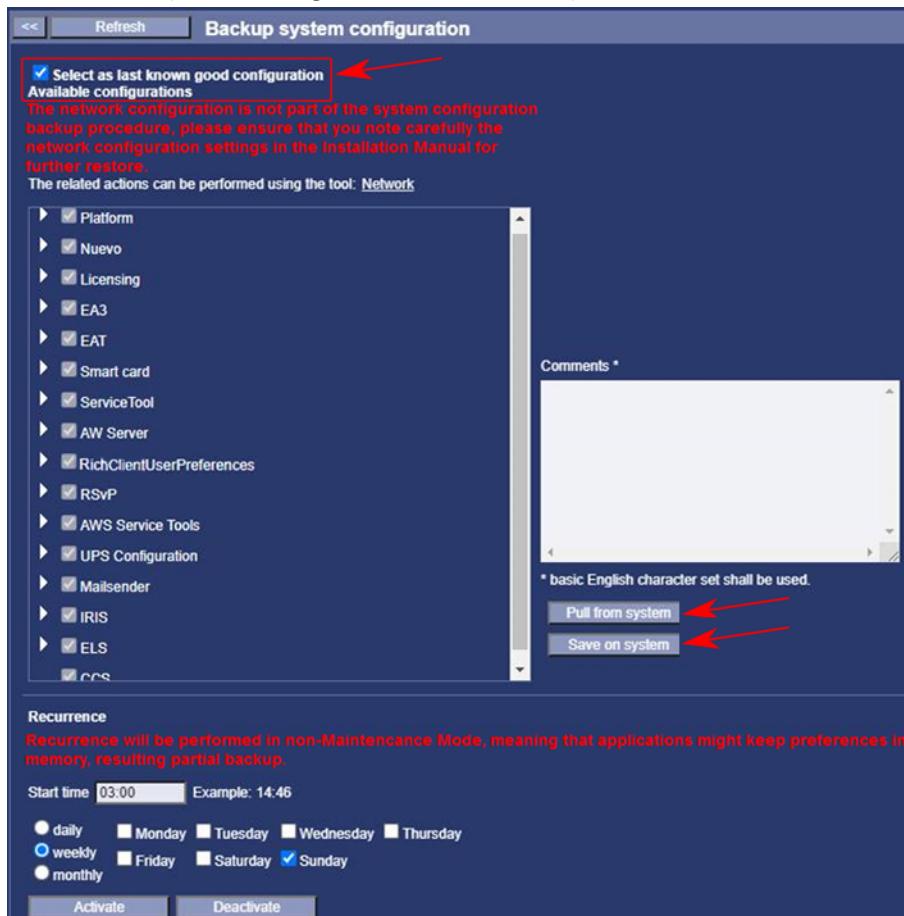
- On physical AW servers with an Image disks array, the backup partition is on the image disks array, so it is normally not affected by the software Load From Cold.
- However for AW Server 2.0 or AW Server 3.0 upgrades, if the customer allows deletion of the existing images, you will choose to upgrade the filesystem from Ext3 to Ext4 for better performances, and consequently, both the Image partition and the Backup partition will be deleted then recreated.
- For AW Server 3.2 Ext. 4.0 or Ext. 4.2 updates, if the external CoLA server(s) IP address(es) have been configured, note down these IP address(es), as they are not saved in the backup and they will need to be added manually while restoring the site configuration.
- For Full, Seamless or DICOM Direct Connect Integration, the backup must be made on the Client PC and/or FE laptop, as reloading the software (OS + AWS) deletes all files on the system hard disk.

## NOTICE

**In all cases, it is strongly recommended to proceed to a double backup**, in order to save the configuration, both on the AW Server by selecting **Save on System** (if applicable), and to a remote location (Client PC and/or FE laptop) by selecting **Pull from system**. You can also copy it to an external media such as USB media for extra security.

- From the Service Tools, select **Maintenance > Backup > System configuration**.

The Backup system configuration menu displays:



- Check the “**Select as last known good configuration**” radio button.
- Proceed with a double backup:
  - Click Pull from system** - This will allow saving the configuration on a USB media, via the Client PC or FE laptop. Follow the instructions on the screen
  - Click Save on System** - This will allow saving the configuration on a dedicated "backup" space on the Server hard disks, which is not erased by the SW load process, unless upgrade from Ext3 to Ext4 filesystem is chosen.

## NOTE

If the Imaging Cockpit components have been installed, a separate backup file related to **CCS** check box and containing the Imaging Cockpit configuration is created. When restoring the system configuration, the Imaging Cockpit configuration file should be restored separately.

### 3.10.3.4 Backup the PACS Integration configuration

**Bypass this step if your AW Server is not integrated.**

The integration mode will not be automatically restored after the software load process. However, there is a "Prefill" utility that can be used. In any case, it is highly recommended to manually backup the Integration configuration parameters.

Refer to [2.19 Job Card IST011 - Integration on page 221](#) and write down the following information that you will need to reinstall the Integration configuration:

I.e: For Seamless integration

- Integration mode : Seamless Integration
- Connector plugin : Dakota Client Library plugin
- License key : license key for Seamless Integration
- Source : [http://<IP address of Universal\\_Viewer\\_server>/services/PacsWebService](http://<IP address of Universal_Viewer_server>/services/PacsWebService)
- Preprocessing user: It is an Universal Viewer user (in our example, we use the default "AWPreProc" user).
- Institute Name: Your site information displayed here.

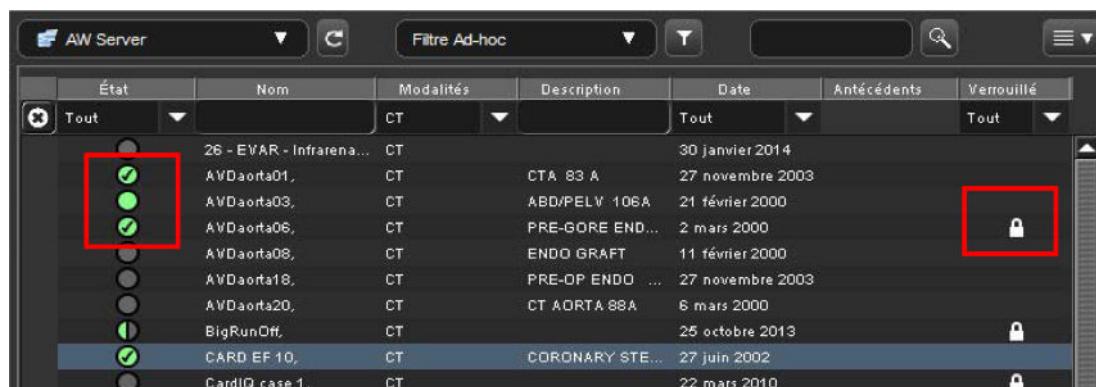
### 3.10.3.5 Backup the existing exams status configuration

**Bypass this step if your AW Server is fully integrated** (Full, Seamless or DICOM Direct Connect Integration).

If the customer requires that part (or all) of the existing patient data is preserved and reinstalled after the upgrade, take a snapshot of the Patients List before proceeding to the upgrade, in order to note which of the exams are locked and/or what is their Post-treatment status.

The database implementation may discard the 'auxiliary tags' or 'meta-data' during a database recover so any configuration done prior to database recovery is lost.

1. If the AW Server has been placed in Maintenance Mode, exit the Maintenance Mode as described in [3.13 Exiting the Maintenance Mode on page 553](#).
2. Replace the AW Server in Maintenance Mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
3. Launch the AW Server Client (login as **service**).
4. Page through the Patients List and write down or make a snapshot of the processed / protected exams.
  - They are flagged with a status symbol and/or a locker symbol.
  - You may need to reset the status and/or re-lock them manually once the upgrade has been done.



État	Nom	Modalités	Description	Date	Antécédents	Verrouillé
Tout	26 - EVAR - Infrarena...	CT		30 janvier 2014		
	AVDaorta01,	CT	CTA 83 A	27 novembre 2003		
	AVDaorta03,	CT	ABD/PELV 106A	21 février 2000		
	AVDaorta06,	CT	PRE-GORE END...	2 mars 2000		
	AVDaorta08,	CT	ENDO GRAFT	11 février 2000		
	AVDaorta18,	CT	PRE-OP ENDO ...	27 novembre 2003		
	AVDaorta20,	CT	CT AORTA 88A	6 mars 2000		
	BigRunOff,	CT		25 octobre 2013		
	CARD EF 10,	CT	CORONARY STE...	27 juin 2002		
	CardIQ case 1,	CT		22 mars 2010		

### 3.10.3.6 Backup the End of Review configuration

For AW Server 2.0 / AW Server 3.1 upgrades to AW Server 3.2 release, it is strongly recommended not to restore the *ServerPreferences.xml* file to avoid potential issue with the Viewer, and this file contains the End of Review configuration. Therefore, backup the EOR configuration as follows:

- Under **Administrative / Configuration** menu, click on **End Of Review** sub-menu and write down the configuration that you will re-create after the software has been upgraded.

### 3.10.4 Software upgrade

Prepare the media that you will use for loading the server with the new version.

Refer to the Software Kit content in section [1.3 Software Kit on page 23](#).

#### NOTE

For the AW Server integrated within the CT/MR Console Environment (Edison HealthLink or CT Console), refer to [2.29 AW Server Integration in CT/MR Smart Subscription on Edison HealthLink on page 307](#) or [2.30 NanoCloud AW Server Installation in CT Console on page 373](#).

#### NOTE

When installing from electronic files, always refer to AW eDelivery Service Guide 5761599-8EN for detailed instructions.

#### NOTE

The Advanced Applications are no longer included in the AW Server Platform software media. They must be loaded from their own media.

#### NOTE

From the AW Server 3.2 Ext. 4.2 release, the system disk size requires 210GB. For the Virtual AW Server the system virtual disk will have to be upgraded from 70GB to 210GB as described later in this section.

#### NOTE

From the AW Server 3.2 Ext. 4.2 release, the system requires additional memories to install Imaging Cockpit components. So, for Virtual AW Server the system virtual memory must be upgraded to 96GB for a Low Tier AW Server and to 104GB for a High Tier AW Server as described later in this section.

This applies only if the Imaging Cockpit components are available for your site (refer to [3.10.4.6 Imaging Cockpit Components installation on page 521](#)).

### 3.10.4.1 Upgrade preparation for Virtual AW Server

#### NOTE

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

1. Open a Web browser and enter the URL or IP address of the ESXi:  
`https://<ESXi URL or IP>/`
2. Login as **service**.
3. To display the list of Virtual Machines, click on **Virtual Machines** on the left side of the page.  
The list of Virtual Machines displays on the right side of the page.

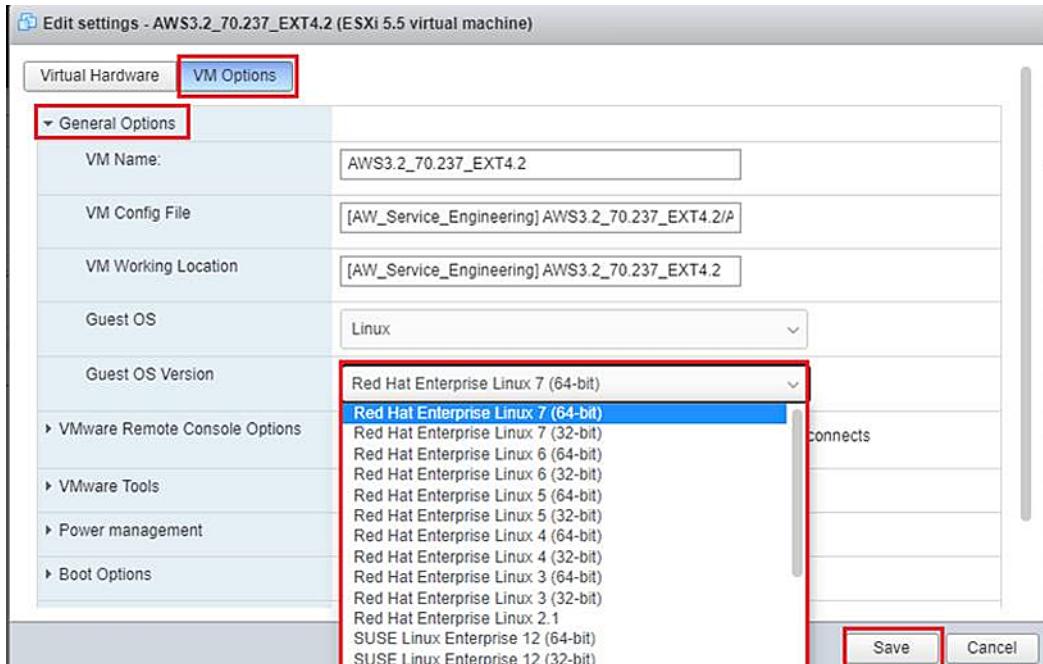
### 3.10.4.1.1 Preliminary step for upgrade from AW Server 3.0 release ONLY

The Guest Operating System information must be changed in **vSphere > Virtual Machine Properties** from **SUSE Linux Enterprise** to **Red Hat Enterprise Linux 7 (64-bit)** prior to proceed to OS upgrade.

1. Select the Virtual Machine and make sure that the VM is powered off.

If not, click on Shut down icon to shut down the guest OS.

2. Select the Virtual Machine, then click on the Edit icon.
3. Select the **VM Options** tab. Select **General Options** line.
4. In **Guest OS**, click on the drop-down list.



5. Select **Red Hat Enterprise Linux 7 (64-bit)**.

6. Select **Save** to apply the new setting.

### 3.10.4.1.2 Upgrade system virtual disk from release prior to AW Server

#### 3.2 Ext. 4.2 ONLY

When upgrading a Virtual AW Server from a release prior to AW Server 3.2 Ext. 4.2, it requires additional disk space on the Virtual Machine. So, the system virtual disk has to be upgraded from 70GB to 210GB.

##### NOTE

This apply to Virtual AW Server other than the Seamless integration.

##### NOTE

**DO NOT MISS THIS STEP!**

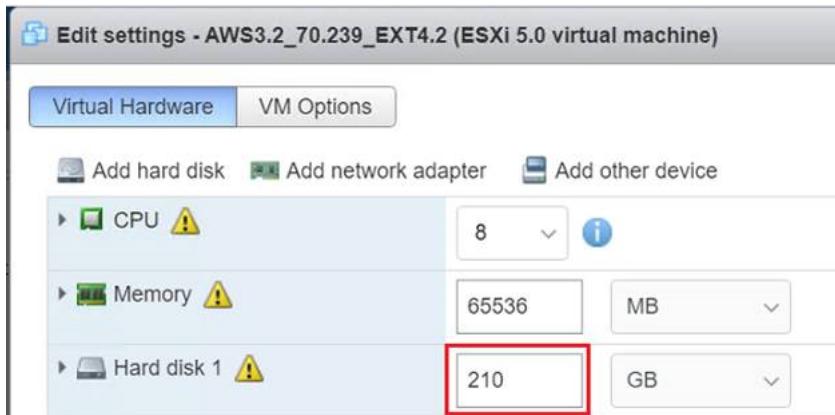
Missing to upgrade the system virtual disk will aboard the AW Server software loading. And the full process should be done again from the OS loading.

1. Select the Virtual Machine and make sure that the VM is powered off.

If not, click on Shut down icon to shut down the guest OS.

2. Click on the Edit icon.

- In the **Virtual Hardware** tab set the **Hard disk 1** size to **210GB**.



- Click on **Save**.

### 3.10.4.1.3 Upgrade system virtual memory from release prior to AW Server 3.2 Ext. 4.2 ONLY

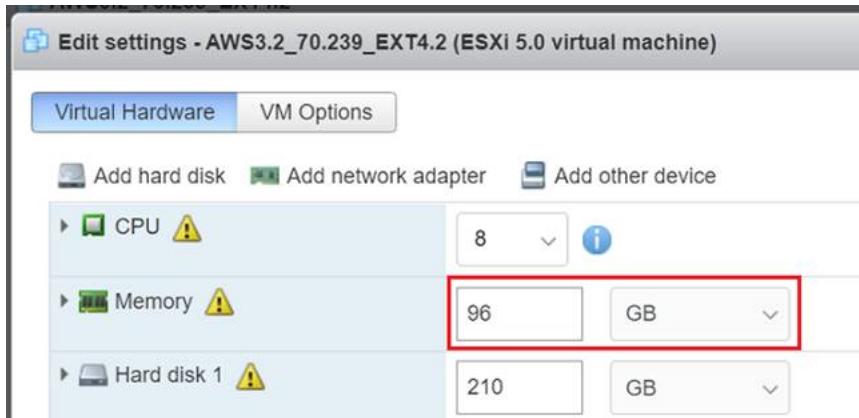
When upgrading a Virtual AW Server from a release prior to AW Server 3.2 Ext. 4.2, it requires additional memory on the Virtual Machine to install the Imaging Cockpit components. So, the system virtual memory must be upgraded to 96GB for a Low Tier AW Server and to 104GB for a High Tier AW Server.

This applies only if the Imaging Cockpit components are available for your site (refer to [3.10.4.6 Imaging Cockpit Components installation on page 521](#)).

- Select the Virtual Machine and make sure that the VM is powered off.

If not, click on Shut down icon to shut down the guest OS.

- Click on the Edit icon.
- In the **Virtual Hardware** tab set the **Memory** to **96GB** for Low Tier AW Server and to **104GB** for High Tier AW Server.



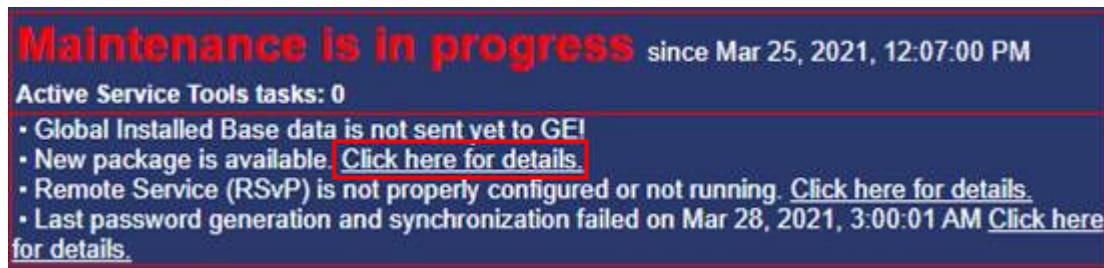
- Click on **Save**.

### 3.10.4.2 Automatic OS and AW Server Platform software installation

For the systems connected via RSvP, if a new version of the AW Server (new version of OS and AW Server Platform software package) is available, it has been automatically loaded onto the AW Server (from the software delivery portal).

This section describes the automatic installation of the AW Server from this package using the **Version Management** page. The steps performed by the automatic installation are:

- Automatic configuration backup.
  - Automatic OS installation.
  - Automatic AW Server platform installation.
  - Automatic configuration restoration.
1. 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.

The **Version Management** page opens.

The screenshot shows the "Server and client side version management" page. At the top, there are tabs for "Install/Uninstall", "Status", and "License Activation". Below that, a sidebar lists "Hard disk", "CD/DVD (/dev/sr0)", and "CD/DVD (/dev/sr1)". At the bottom of the sidebar are buttons for "Contents", "Upload ISO", and "Upload DVD Collector".

The main area is divided into two sections:

Currently installed	Available for installation on Hard disk						
<b>OS, Platform</b> OS: Scientific Linux release 7.9 (Nitrogen) Platform: AW Server aws-3.2-4.8-2219.2-22420c6b	OS: Scientific 7.9 AWS3.2_OS_7.1-2218.5- <input checked="" type="checkbox"/> 0c430548 Platform: AW Server aws-3.2-4.8-2220.1-bdb1db43						
<b>Enterprise Cockpit and Web Applications</b>	No package available for installation						
<b>Applications</b>	<table border="1"> <tr> <td><input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details</td> <td>2/70</td> <td><input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details</td> </tr> <tr> <td></td> <td></td> <td><input type="checkbox"/> Advantage 4D 2.3.600 ► Details</td> </tr> </table>	<input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details	2/70	<input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details			<input type="checkbox"/> Advantage 4D 2.3.600 ► Details
<input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details	2/70	<input type="checkbox"/> Volume Viewer Apps 16.0-6.76 ► Details					
		<input type="checkbox"/> Advantage 4D 2.3.600 ► Details					

At the bottom, there are buttons for "Uninstall", "Install" (which is highlighted with a red box), "Don't install", and "Remove package".

2. If the  icon is present in front of the new OS and AWS Platform package name, click on it to view the related installation instructions. In any case, use the latest Installation Manuals, from the SIMS Content viewer, to have the latest installation procedures.

#### NOTE

The  icon means that the package has been automatically loaded from the software delivery portal.

3. Select the OS and AW Server Platform package and click on **Install**.
4. In the popup that displays, click on **OK** to confirm the automatic installation.
5. In the popup that displays, click on **OK** to automatically perform a full system configuration backup.

- Acknowledge the next popups that display.

**NOTE**

The security Hardening will be reapply later in the upgrade procedure.

- The installation can take several minutes (up to 60 minutes) to complete. Regularly relaunch the Service Tools, as they will restart once the installation is complete.

Go to section [3.10.4.6 Imaging Cockpit Components installation on page 521](#).

### 3.10.4.3 OS installation

The OS software is delivered either:

- In the [Physical Software Kit on page 23](#). Use the following file:

Part Number	Content	Purpose	AWS Type	Integration Mode
5872674-6 (or higher)	 AWS3.2_OS_7.2-Scientific-7.9.iso	This iso file is used for <b>Upgrade/Update</b> . It contains the OS (Scientific Linux 7.9).	Virtual Physical	No-integ Hybrid Seamless DDC

**NOTE**

The reference checksum file (.sha256 extension) is not listed in the table. However, it is present in the USB media to verify file integrity.

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use the following file to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	AWS Type	Integration Mode
5865571-3_Operating_System_AWS3.2_OS_Rev.7.2_for_AW_Server_3.2.iso	This iso file is used for <b>Upgrade/Update</b> . It contains the OS (Scientific Linux 7.9).	Virtual Physical	No-integ Hybrid Seamless DDC

**NOTE**

The reference checksum, to verify file integrity, is listed in the *packagemetadata.json* file.

**NOTE**

When installing from electronic files, always refer to [5761599-8EN AW eDelivery Service Guide](#) for detailed instructions.

#### 3.10.4.3.1 Physical AW Server

The steps are done at the Server side. Alternatively, software loading can also be done at the Client PC, through the iLO service processor. Refer to [A.6 Software Loading Through iLO on page 579](#).

- Power up the system:

After a while, the screen unblanks and displays the HP ProLiant logo. Next the boot up messages are displayed. It takes some time for the system to initialize. Please be patient.

- Insert the DVD or the USB media into the server.

- Reboot the AW server:

At the KVM or at the Client PC, login as **root**.

Type:

**reboot <Enter>**

The server reboots. After a while, the screen unblanks and displays the HP ProLiant logo, followed by other boot up messages.

**NOTICE**

If hardware security has been activated on this hardware, the system will directly attempt to boot from the hard disk. Therefore you should first press on the **<F11>** key when prompted, to enter the boot device selection. You will be prompted to enter the BIOS Administrator password (if you have setup one) for the server hardware security (see AW Server 3.2 Hardware Installation Manual, section *Hardware failure upon installation* and *Hardware lockup for security*) to gain access to the boot menu.

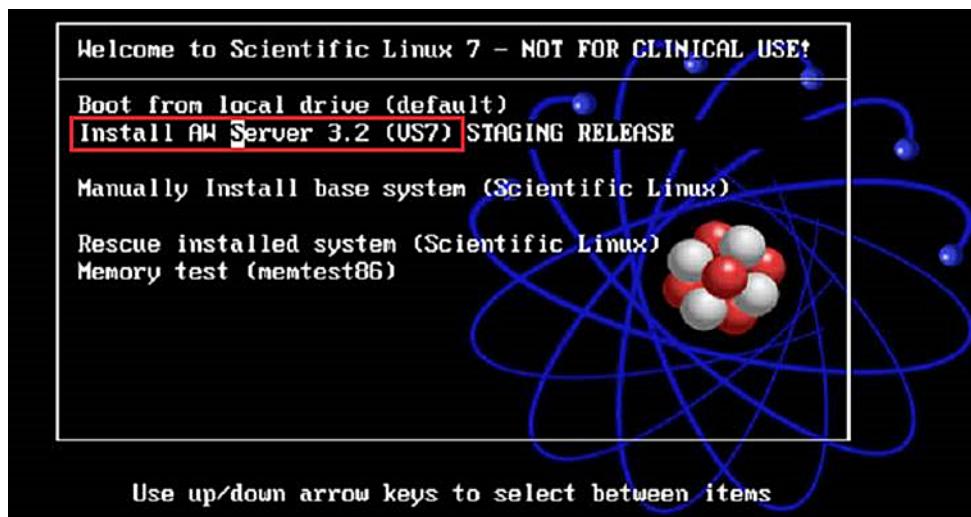
It will take a few moments before you get to the boot selection menu screen. Please be patient. When done, select **One time boot to CD-ROM or USB**.

**NOTE**

If you lost the BIOS Administrator password, refer to AW Server 3.2 Advanced Service Manual 5771771-8EN, Chapter 9, Appendix A.24.

4. *Scientific Linux* menu displays:

The message *Attempting to boot from CD-ROM* will display, followed by the *Welcome to Scientific Linux* menu screen:



Use the **<Up arrow>** and **<Down arrow>** keys to select **Install AW Server 3.2 (VS7)** and press **<Enter>**.

**NOTE**

If you do not select anything, within about 10 seconds, it would result to boot from the local drive. In this case cycle power to the AW Server in order to reboot, and select **Install AW Server 3.2 (VS7)**.

5. Lots of messages display followed by the installation start screen:

```
Starting installer, one moment...
anaconda 21.48.22.147-1 for HELiOS 7.6SP1 started.
* installation log files are stored in /tmp during the installation
* shell is available on TTY2
* when reporting a bug add logs from /tmp as separate text/plain attachments
13:13:30 Running pre-installation scripts
13:13:32 Not asking for VNC because of an automated install
13:13:32 Not asking for VNC because text mode was explicitly asked for in kickstart
13:13:32 Not asking for VNC because we don't have a network
Starting automated install.....
Checking software selection
-
```

[anaconda] 1:main\* 2:shell 3:log 4:storage-lo> Switch tab: Alt+Tab | Help: F1

6. Then the packages installation will start:

```
Installing lz4.i686 (1127/1148)
Installing libtasn1.i686 (1128/1148)
Installing libattr.i686 (1129/1148)
Installing libcap.i686 (1130/1148)
Installing systemd-libs.i686 (1131/1148)
Installing dbus-libs.i686 (1132/1148)
Installing avahi-libs.i686 (1133/1148)
Installing cups-libs.i686 (1134/1148)
Installing qt.i686 (1135/1148)
Installing qt-x11.i686 (1136/1148)
Installing gtk2.i686 (1137/1148)
Installing gnutls.i686 (1138/1148)
Installing libcurl.i686 (1139/1148)
Installing mesa-libGLU.i686 (1140/1148)
Installing pygobject2.i686 (1141/1148)
Installing libXaw.i686 (1142/1148)
Installing motif.i686 (1143/1148)
Installing qt3.i686 (1144/1148)
Installing libXtst.i686 (1145/1148)
Installing libXScrnSaver.i686 (1146/1148)
Installing libxml2.i686 (1147/1148)
Installing libgomp.i686 (1148/1148)
Performing post-installation setup tasks
```

[anaconda] 1:main\* 2:shell 3:log 4:storage-lo> Switch tab: Alt+Tab | Help: F1

It takes about 10 to 15 minutes to install the packages.

7. When that is done, system starts rebooting.

The server will initialize, then the *Scientific Linux* menu will display. After a few seconds, the system will automatically boot up from the hard disks.

When the boot up sequence has completed you will be prompted to login and enter the login password.

8. Eject the OS DVD or remove the USB media and store it in a safe place.

Operating System (OS) load is complete.

9. Insert the AWS platform DVD or insert the USB media containing the AWS Platform software.

Go to section [3.10.4.4 AW Server Platform software installation on page 517](#).

### 3.10.4.3.2 Virtual AW Server

The steps are done at the Client PC.

#### NOTE

The steps are described for **VMware** hypervisor (ESXi) with **VMware vSphere Web Client**. If needed, refer to VMware documentation for more details.

For a description with **Microsoft** hypervisor (Hyper-V), refer to the corresponding documentation.

1. Insert the media into the Client PC.
2. Display the Virtual Machine Console and start the virtual machine:
  - Click on the Console screen shot (here the white arrow if the Virtual Machine is not already started).

The virtual AW Server OS starts booting up (if not already started) and the Virtual Machine Console opens.



#### NOTE

Once the virtual machine is started, you can also display the Virtual Machine Console by clicking on **Console > Open browser console** or directly on the Console screen shot.

#### NOTE

To work with the Virtual Machine Console, simply click into the console field.

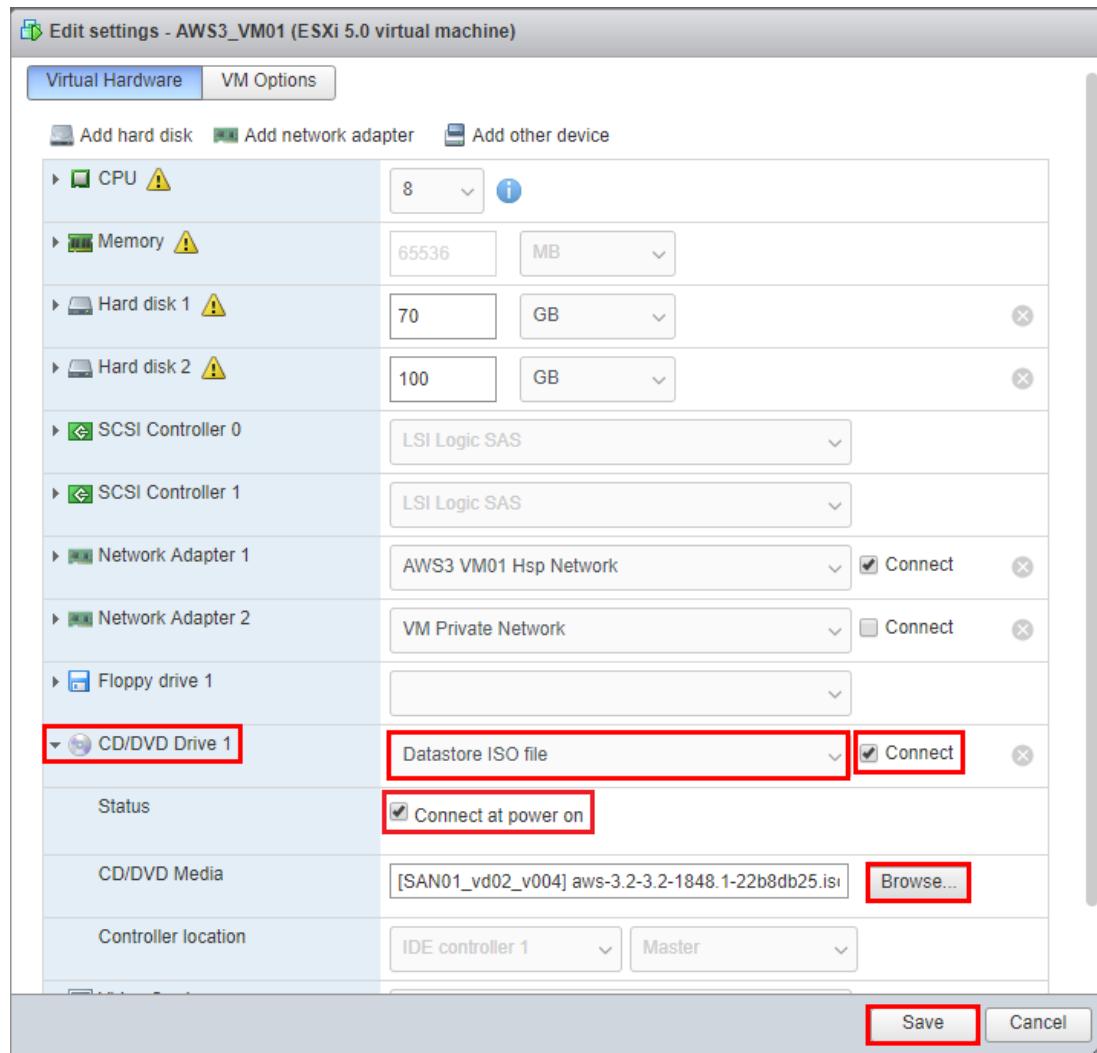
If the screen is black or locked press **<Ctrl>**.

To display the boot sequence while booting press **<Ctrl>** and **<->** simultaneously.

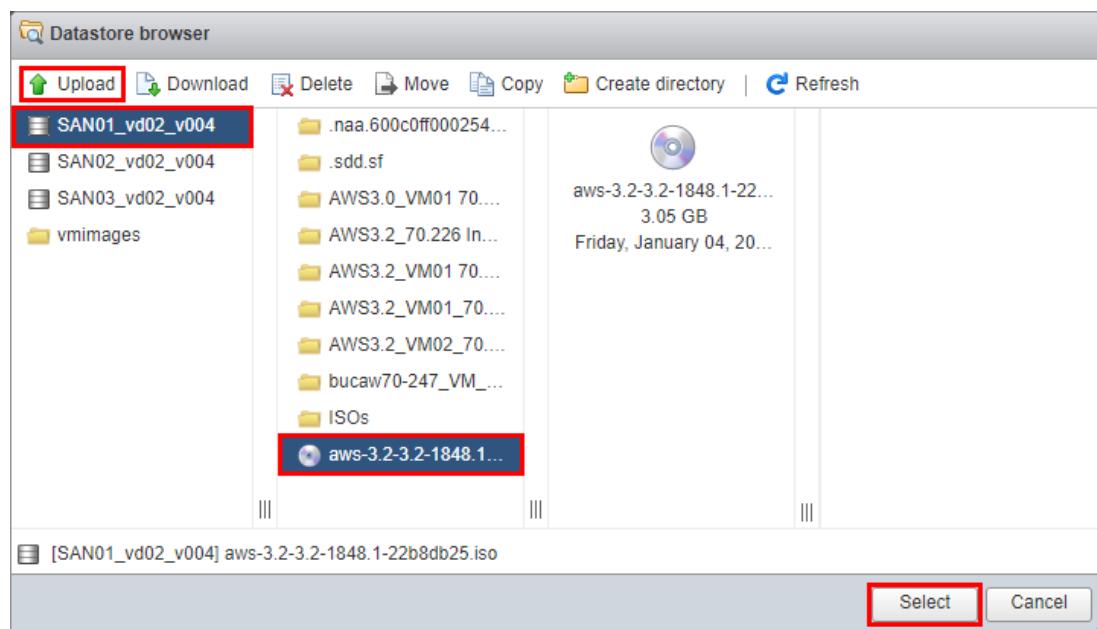
3. Map the iso file to the virtual CD/DVD drive:

- Select your Virtual Machine, then click on the **Edit** icon.

The *Edit settings* screen displays.



- In the **Virtual Hardware** tab select **CD/DVD Drive 1** (or the corresponding name for your VM) from the list.
- If not already selected, select **Datastore ISO file** from the dropdown list. Otherwise, click on the **Browse...** button.
- In the screen that displays:



- If the iso file is not already uploaded:
  - Select the datastore where you want to copy the iso file and click on **Upload**.
  - Locate the iso file and select it, then select **Open**.
- Once uploaded, select the iso file and click on **Select** button.
- In the *Edit settings* screen check the **Connect at power on** and the **Connect** radio buttons.
- Click on **Save** button.

The virtual CD/DVD drive of the Virtual Machine is now mapped to the iso file.

#### 4. Reboot the AW server:

Log into the Console as **root**.

Type:

**reboot <Enter>**

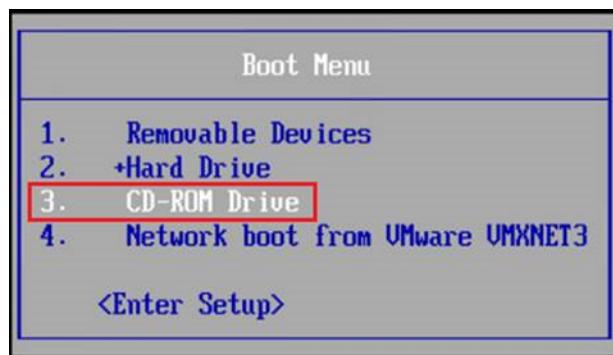
#### NOTICE

**IMPORTANT - To force boot from the CD** rather than from the Hard Disk, when proceeding to software Load from Cold, at the start of the boot sequence, **quickly press "Esc"** when the VMware logo briefly displays at the Console. This will launch the boot menu, from were you can choose to boot from "CD-Rom Drive" and select "Connect to ISO image on local disk".

#### NOTE

The Console remains black for about 30 seconds before the start of the boot sequence appears.

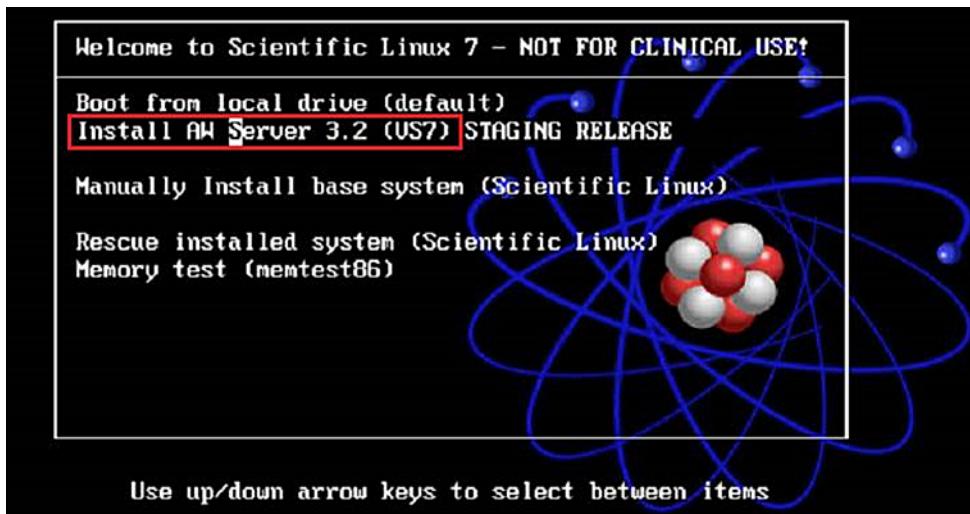
#### 5. The Boot Menu displays:



Use the **Up arrow** and **Down arrow** keys to select **CD-ROM Drive** and press **Enter**.

#### 6. Scientific Linux menu displays:

The message **Attempting to boot from CD-ROM** will display, followed after a moment by the *Scientific Linux* menu screen:



Use the **<Up arrow>** and **<Down arrow>** keys to select **Install AW Server 3.2 (VS7)** and press **<Enter>**.

## NOTE

If you do not select anything, within about 10 seconds, it would result to boot from the local drive. In this case cycle power to the AW Server in order to reboot, and select **Install AW Server 3.2 (VS7)**.

7. Lots of messages display followed by the installation start screen:

```
Starting installer, one moment...
anaconda 21.48.22.147-1 for HELIOS 7.6SP1 started.
* installation log files are stored in /tmp during the installation
* shell is available on TTY2
* when reporting a bug add logs from /tmp as separate text/plain attachments
13:13:30 Running pre-installation scripts
13:13:32 Not asking for VNC because of an automated install
13:13:32 Not asking for VNC because text mode was explicitly asked for in kickstart
13:13:32 Not asking for VNC because we don't have a network
Starting automated install.....
Checking software selection
-
```

8. Then the packages installation will start:

```

Installing lz4.i686 (1127/1148)
Installing libtasn1.i686 (1128/1148)
Installing libattr.i686 (1129/1148)
Installing libcap.i686 (1130/1148)
Installing systemd-libs.i686 (1131/1148)
Installing dbus-libs.i686 (1132/1148)
Installing avahi-libs.i686 (1133/1148)
Installing cups-libs.i686 (1134/1148)
Installing qt.i686 (1135/1148)
Installing qt-x11.i686 (1136/1148)
Installing gtk2.i686 (1137/1148)
Installing gnutls.i686 (1138/1148)
Installing libcurl.i686 (1139/1148)
Installing mesa-libGLU.i686 (1140/1148)
Installing pygobject2.i686 (1141/1148)
Installing libXaw.i686 (1142/1148)
Installing motif.i686 (1143/1148)
Installing qt3.i686 (1144/1148)
Installing libXtst.i686 (1145/1148)
Installing libXScrnSaver.i686 (1146/1148)
Installing libxml2.i686 (1147/1148)
Installing libgomp.i686 (1148/1148)
Performing post-installation setup tasks
[anaconda] 1:main* 2:shell 3:log 4:storage-> Switch tab: Alt+Tab | Help: F1

```

It takes about 10 to 15 minutes to install the packages.

9. When that is done, the system starts rebooting.

The server will initialize, then the Scientific Linux menu will display. After a few seconds, the system will automatically boot up from the hard disks.

When the boot up sequence has completed you will be prompted to login and enter the login password.

10. Remove the USB media and store it in a safe place.

Operating System (OS) load is complete.

11. Disconnect the iso file from the CD/DVD virtual drive:

- Select the Virtual Machine, then click on the  icon.
- The Edit settings screen displays.
- In the *Virtual Hardware* tab, in front of **CD/DVD Drive 1** (or the corresponding name for your VM) uncheck the **Connect** radio button.
  - Click on the **Save** button.
  - The following message displays:
- "The guest operating system has locked the CD-ROM door..."
- Select the **Yes** check box then click on the **Answer** button.
- Go to section [3.10.4.4 AW Server Platform software installation on page 517](#).

### 3.10.4.4 AW Server Platform software installation

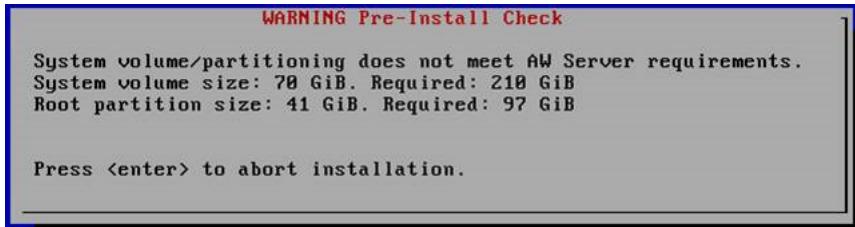
Proceed with the AWS platform loading steps described at chapter 2, [2.11 Job Card IST003 - Installation of Platform Software on page 109](#).

You will be prompted to choose between preserving the existing images (and potentially remaining in Ext3 filesystem type: AW Server 2.0 / 3.0 case), or allowing deletion of the existing images and upgrading to Ext4 filesystem (faster type).

When done, continue with the following steps.

## NOTICE

While loading the AW Server software, if the below warning pops up, it means that the system virtual disk has not been upgraded. In this case, upgrade the system virtual disk as described in [3.10.4.1.2 Upgrade system virtual disk from release prior to AW Server 3.2 Ext. 4.2 ONLY on page 507](#) and reload the OS as described in [3.10.4.3 OS installation on page 510](#).



## 3.10.4.5 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

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.

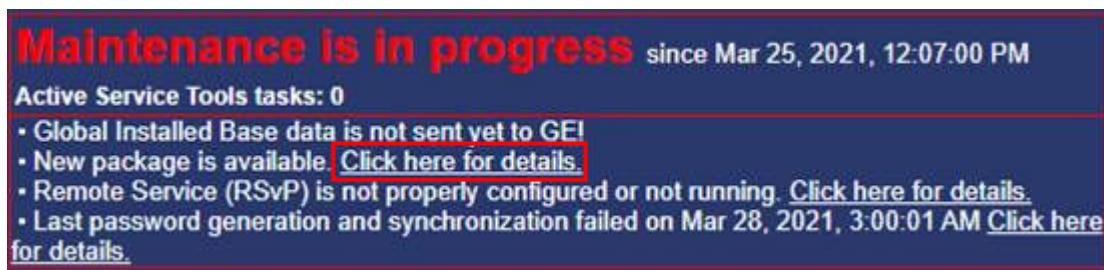
### NOTE

It is **not** possible to uninstall a Service Pack.

### 3.10.4.5.1 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 [3.10.4.5.2 Installing the OS and AW Server Platform software Service Pack on page 520](#).

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.

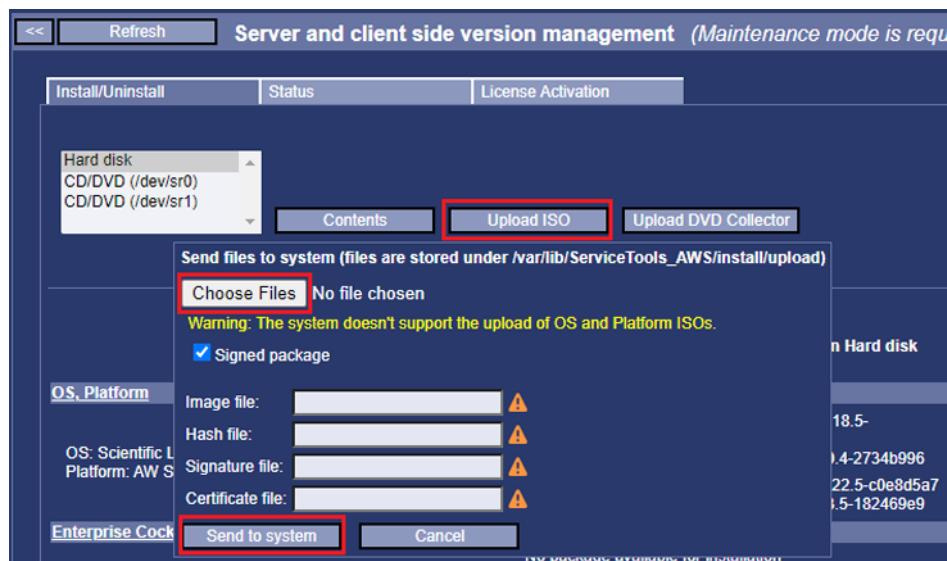
1. Insert the AW Server Service Pack media into the Client PC or the FE laptop.
2. From the Service Tools, select **Maintenance > Version Management**.
3. Carefully read the warning message that appears and make sure you understand it prior to click on **OK** to close the message.
4. Click on **Upload ISO**.
5. If the Service Pack ISO file is **signed**, follow the below substeps. Otherwise, jump to next step.

**NOTE**

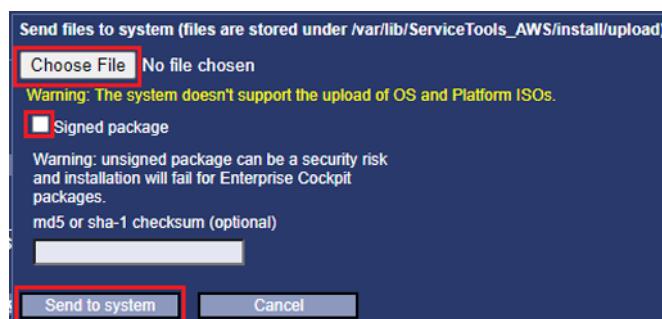
A signed ISO is composed of 4 files: the ISO itself and an hash, a signature and a certificate files which are used to check the authenticity of the ISO file.

If the Secured for RMF mode is planned to be activated, only signed ISO is accepted.

- a. 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).



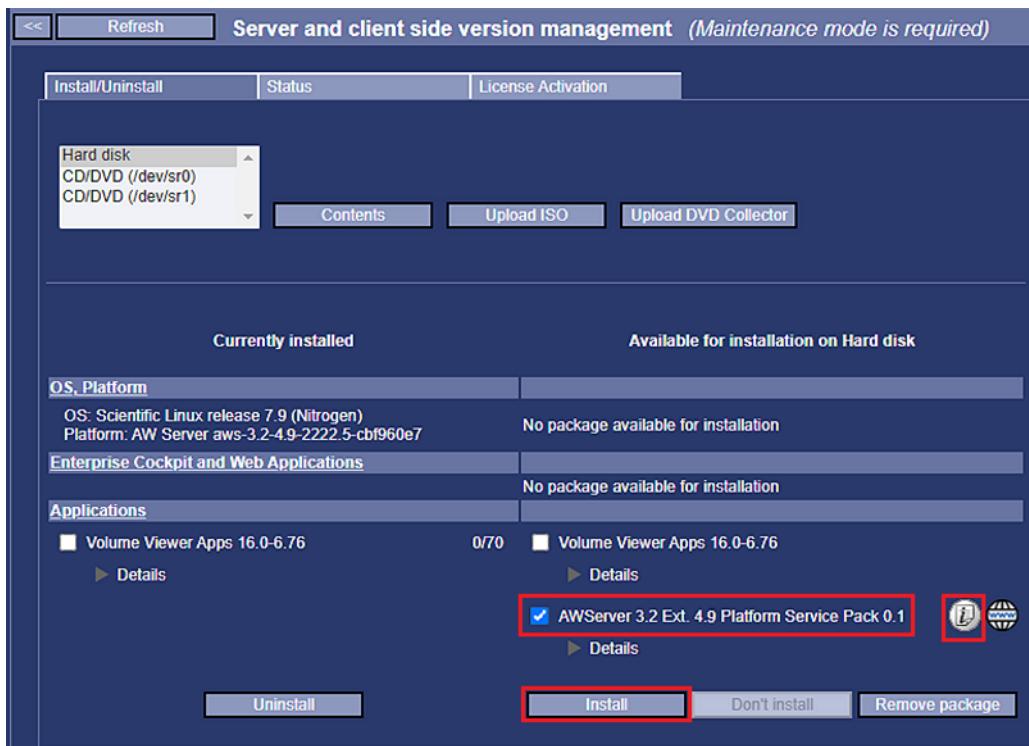
- b. The **Image file** (Service Pack ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
6. If the Service Pack ISO file is **not signed**, follow the below substeps.
  - a. In the pop-up window, uncheck the **Signed package** check box.
  - b. Click on **Choose File** and select the ISO file stored on the media.



- c. 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.
7. To upload the ISO file click on **Send to system**.
- When the upload is completed, acknowledge the popup that displays.
8. Verify that the Service Pack appears in the Available for installation on Hard disk part of the page.
9. Remove the media from the Client PC or FE laptop.

### 3.10.4.5.2 Installing the OS and AW Server Platform software Service Pack

1. 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.

2. 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.
3. Select the **Install/Uninstall** tab.
4. Check that the AW Server Service Pack appears in the **Currently installed** part of the page.

5. On the Healthpage, in **System Configuration** table, the **Modality OS Version** is updated.

Operating System	Scientific Linux release 7.9 (Nitrogen)
OS Version	7.9
Modality OS Version	AWS3.2_OS_7.2_SP_1.0 [20230109]
UDI	(01)00840682102384(10)AWS03D02E4D9SP1D0

6. Reboot the AW Server.

From the Service Tools, select **Tools > Reboot**, then select **Reboot AW Server**.

Wait for the AW Server to reboot, then login again into the Service Tools.

On the Healthpage, the **AWS Service Pack Version** displays in **Version Information**.

Version Information	
AWS Service Pack version	aws-sp-3.2.4.9-1.0

#### NOTE

If any issue occurs during the Service Pack installation or if the system does not work as expected after the Service Pack installation:

- Report the issue and contact an Online Service Engineer to collect the logfiles for further investigation.
- Use the backup created prior to install the Service Pack and reload the current AW Server (as for an upgrade – Load From Cold).

### 3.10.4.6 Imaging Cockpit Components installation

The Imaging Cockpit introduces AW Server platform components that allows using a web-based AW Server Client (Web Client) to start the advanced applications.

The Imaging Cockpit is supported on the following AW Server configurations:

Tier	HW platform	Slice count license	No-Integ	Hybrid	Seamless (UV)	DICOM Direct Connect (DDC)
Physical LT	HP DL360 – G10	40k - SdC_Low_Tier_Premium	X	X		
Physical HT	HP DL360 – G10	80k - SdC_High_Tier_Standard	X	X		X
		160k - SdC_High_Tier_Premium	X	X		X
	HP DL360 – G9	80k - SdC_High_Tier_Standard	X	X		
		160k - SdC_High_Tier_Premium	X	X		
VM LT	Any	40k - SdC_Low_Tier_Premium	X	X		X (without clustering)
VM HT	Any	40k - SdC_Server_Eight_Seats	X	X		X

#### NOTE

If the Secured for RMF mode needs to be activated, then **do not perform** this procedure.  
Imaging Cockpit and AW Server Web client are not supported in RMF mode.

#### NOTE

The Web Client requires a license to be activated.

Refer to [2.15.10.5 Flexera licensing on page 162](#). If it is available for your site, it will be restored later in this upgrade procedure.

**NOTE**

No DICOM communication is possible between Web Client and a remote DICOM host in the **192.168.x.x** IP address range.

The Imaging Cockpit Components available for upgrade are within:

- Edison Machine Light and Services
- Imaging Fabric
- Enterprise Cockpit Web Client

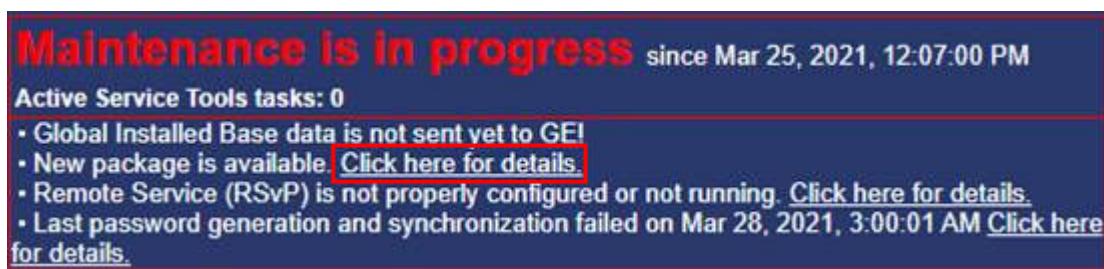
**NOTE**

The DNS setting is mandatory for the Imaging Cockpit environment. In case the site's DNS server(s) have not been set up during the early installation, they can be configured through the Service Tools, as described in [A.8.8 DNS server\(s\) setup - Alternate method on page 594](#).

### 3.10.4.6.1 Loading the Imaging Cockpit Components

For the systems connected via RSvP, if new Imaging Cockpit Components (ISOs files) are available, they have 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 [3.10.4.6.2 Installing the Imaging Cockpit Components on page 524](#).

The Imaging Cockpit Components are delivered either:

- In the [Physical Software Kit on page 23](#). Use the following files:

Part Number	Content	Purpose	AWS Type	Integration Mode
5872674-6 (or higher)	aws-eml-1.12.0.iso	These iso files are used for <b>Initial Installation &amp; Upgrade/Update</b> .  They contain the Imaging Cockpit Components: <ul style="list-style-type: none"> <li>• Edison Machine Light and Services</li> <li>• Imaging Fabric</li> <li>• Enterprise Cockpit Bundles</li> </ul>	Virtual Physical	No-integ Hybrid DDC
	aws-if-1.7.2.iso			
	aws-ec-1.3.0.iso			

- In the [Digital Software Kit \(files downloaded via eDelivery\) on page 25](#). Use the following files to prepare the USB media with the AW eDelivery Install Manager (AWeDIM) tool:

File name (in eDelivery Software Portal)	Purpose	AWS Type	Integration Mode
5865567-5_AW_Server_Edison_Machine_Light_and_Services_1.12.0.zip	These compressed packages are used for <b>Initial Installation &amp; Upgrade/Update</b> .  It contains the Imaging Cockpit Components.	Virtual Physical	No-integ Hybrid DDC
5865565-5_AW_Server_Imaging_Fabric_Component_1.7.2.zip			
5865569-5_AW_Server_Enterprise_Cockpit_Components_1.3.0.zip			

**NOTE**

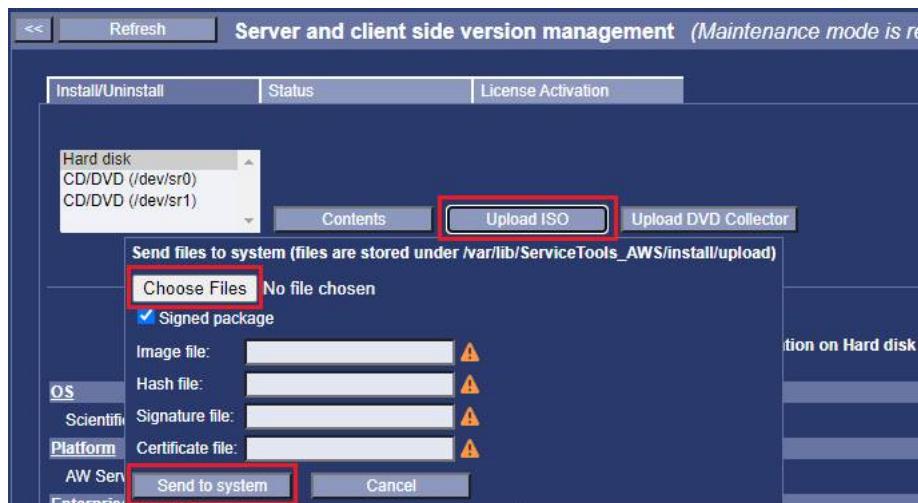
When installing from electronic files, always refer to *5761599-8EN AW eDelivery Service Guide* for detailed instructions.

1. Insert the 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**.

**NOTE**

The components ISO files are signed. This means that each component 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.

5. In the pop-up window click on **Choose File** and select the component 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).



6. The **Image file** (component ISO file), **Hash file**, **Signature file** and **Certificate file** fields get populated with the files selected.
7. To upload the ISO file click on **Send to system**.
8. Once loaded, click on **OK** in the popup that displays.
9. Verify that the component appears in the *Available for installation on Hard disk* part of the page.
10. To load the other components, proceed as in **Step 4 to Step 9**.

11. Remove the media from the Client PC or FE laptop.

**NOTE**

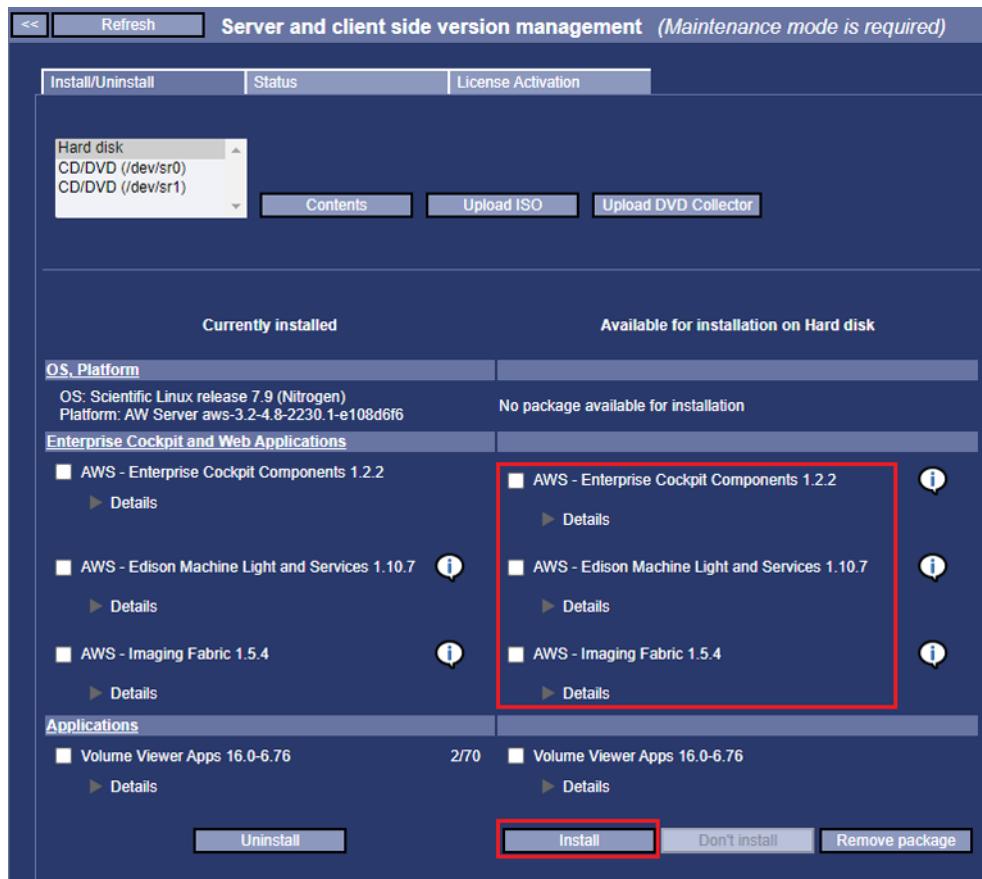
To remove a component, in the *Available for installation on Hard disk* part of the page, click to select the radio button corresponding to the component you want to remove from the AW Server hard disk and click on the **Remove package** button.

### 3.10.4.6.2 Installing the Imaging Cockpit Components

**NOTE**

If the Edison Machine Light and Services component is ready to be installed, always start with this component.

1. Select the **Edison Machine Light and Services** component and click on **Install**.



**NOTE**

For the systems connected via RSvP, if new components versions are available, they have been automatically loaded onto the AW server (from the software delivery portal), and the icon is displayed in front of the components name. If installation instructions are available, the icon is also present in front of the component name. Click on it to review the instructions.

2. In the pop-up window, click on **OK** to proceed with installation.

The installation status page displays the installation steps.

**NOTE**

It will take several minutes to complete. Up to 10 minutes to install a component.

3. When the installation is completed, click on **OK** in the window that pops up.

4. Install the other components.

Proceed as in steps [Step 1 to Step 3](#), to install the **Imaging Fabric** and the **Enterprise Cockpit Web Client** components.

5. Select the **Install/Uninstall** tab and verify that the component(s) appears in the *Currently installed* part of the page.

### 3.10.4.7 Loading the HPE R/T3000 UPS drivers and restoring the configuration (if applicable)

The HPE R/T3000 UPS utility driver is part of the AWS Platform software, and is automatically loaded and installed when loading the AWS software from media.

The following steps are normally performed by connecting to the server locally, from the server KVM.

If you remotely connect from another computer, disable the server's PNF firewall before connecting.

#### NOTE

Customer's owned UPS configuration case: If applicable for your site, restore the customer's UPS configuration as specified by the IT administrator of the site.

1. Open a terminal window from the **Tools > Terminal** menu option and login as **root**.
2. Disable the firewall:

```
systemctl stop pnf <Enter>
```

3. Check that the HPE R/T3000 UPS driver has been properly installed on the system as described in [2.12.1 HPE R/T3000 UPS drivers installation verification on page 124](#).

4. If you did NOT modify the default HPE R/T3000 UPS configuration:

Proceed with [2.12.2 Configuring the HPE R/T3000 UPS using HPPP Software on page 124](#), to reconfigure the HPE R/T3000 UPS auto-shutdown parameters.

5. If you have modified the default HPE R/T3000 UPS configuration (I.e: you changed the default 10mn delay time before shutdown to any other value), restore the configuration from the HPE R/T3000 UPS backup file:

- a. Restore the HPE R/T3000 UPS configuration (if applicable):

- ```
systemctl stop HP-HPPP <Enter>
cd /export/backup/ups <Enter>
cp config.js /usr/local/HP/PowerProtector/configs <Enter>
cp mc2.db /usr/local/HP/PowerProtector/db <Enter>
```
- Or use the File Transfer tool if you have saved the configuration on Client PC or FE laptop (Load From Cold case). Select the **To system** tab to transfer the `config.js` and the `mc2.db` files to the `configs` and `db` directories as shown above.

```
systemctl start HP-HPPP <Enter>
```

- b. To test the shutdown utility and make sure it is operational, refer to [Step 14](#) in [2.12.2 Configuring the HPE R/T3000 UPS using HPPP Software on page 124](#).

6. Enable the firewall back:

```
iptables -F <Enter>
```

```
systemctl start pnf <Enter>
```

## 3.10.5 Reload and reinstall the Advanced Applications

### 3.10.5.1 Information about Volume Viewer Applications

See [2.17.5 Applications Profile on page 182](#) for the list of supported Volume Viewer Applications.

### 3.10.5.2 Information about other Applications

See [2.17.5 Applications Profile on page 182](#) for the list and version of the other supported Applications.

Refer to the dedicated documentation of the Applications for details.

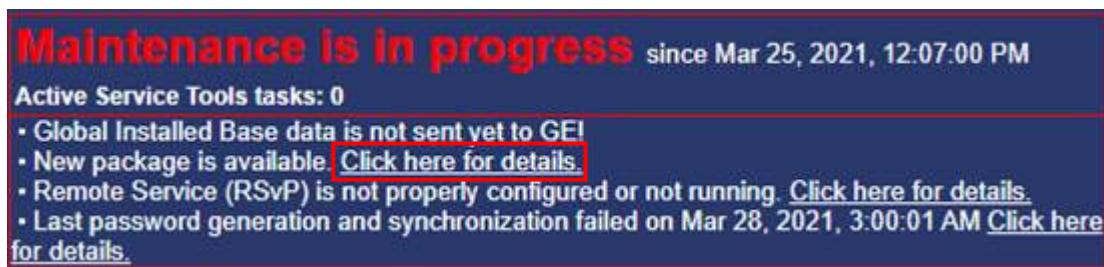
### 3.10.5.3 Applications re-installation and upgrade process

After a Load From Cold, the Applications purchased by the site shall be reloaded and reinstalled from their media.

If new versions of the Applications are available load and install these new versions.

For the systems connected via RSvP, if new Application(s) are available, they have 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 Install the Application - perform the steps in [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#) - [2.17.3 Install the Application\(s\) on page 178](#).

Otherwise, the Applications are available either:

- From the Applications media.
- Have been copied to USB media through the eDelivery mechanism.

#### NOTE

When loading from electronic files, always refer to 5761599-8EN AW eDelivery Service Guide for detailed instructions.

Perform the steps described in [2.17.2 Load the Application\(s\) from media on page 174](#) and [2.17.3 Install the Application\(s\) on page 178](#).

#### NOTE

Bypass CardIQ Xpress Process (CXP) reinstallation, as the Pre-requisite for CardIQ Xpress Process installation are that Volume Viewer, CardIQ Xpress Reveal and Pre-processing are licensed and installed. This is not the case yet. CXP license must also be set before installing the CXP package.

## 3.10.6 Restore the Server configuration and licenses

### NOTE

On an AW Server with Secured for RMF mode activated only backup created in RMF mode will be allowed to restore.

### 3.10.6.1 Preliminary steps before restoration

#### 1. Applications reinstallation

- CardIQ Xpress Process (CXP) application shall be reloaded later, after all CXP install prerequisites are complete and the licenses have been restored. See section [3.10.6.4 CardIQ Xpress Process \(CXP\) application reinstallation on page 531](#).

#### 2. Seamless Integration plugin reinstallation

### NOTICE

Prior to restore the configuration, if your system is in Seamless Integration with the Universal Viewer, it is necessary to reload the latest Dakota plugin.

- Refer to section [2.19.3.4 Seamless integration - configuration steps on AWS, Service Tools on page 231](#).

#### 3. User passwords restoration

### NOTICE

It is not possible to restore the User passwords from AWS2.0 / AWS3.0 to AW Server 3.2. The algorithm used for /etc/shadow file is different between SuSE OS and Scientific Linux OS.

- If you have previously changed the system user passwords (e.g. root, filetransfer) for your site, they will not be restored (upgrade case) and therefore you will have to change them again.

### 3.10.6.2 Restoration steps

Restore now the system configuration files and user preference files.

This is done through the Restore tool in the Maintenance menu. This is one of the server maintenance activities locked into the Maintenance Mode – to ensure corruption-free configuration files – and CAN BE PERFORMED ONLY IN MAINTENANCE MODE

1. When selecting the configuration backup file, take into account the following limitations of the Configuration Restore feature:

- a. For systems where the secured mode was not yet selected (only during a fresh installation scenario): all types of backups (i.e. created in **Generic Hardening** mode or created in older configurations without any type of hardening or created in **Secured for RMF** mode) shall be accepted.
  - AW Servers where backups created in **Generic Hardening** mode or older configurations without any type of hardening were restored, shall be configured only to **Generic Hardening** mode afterwards.
  - AW Servers where backups created in **Secured for RMF** mode were restored, shall be configured only to **Secured for RMF** mode afterwards.
- b. For AW Servers with **Secured for RMF** active shall only accept backups created in **Secured for RMF** systems.

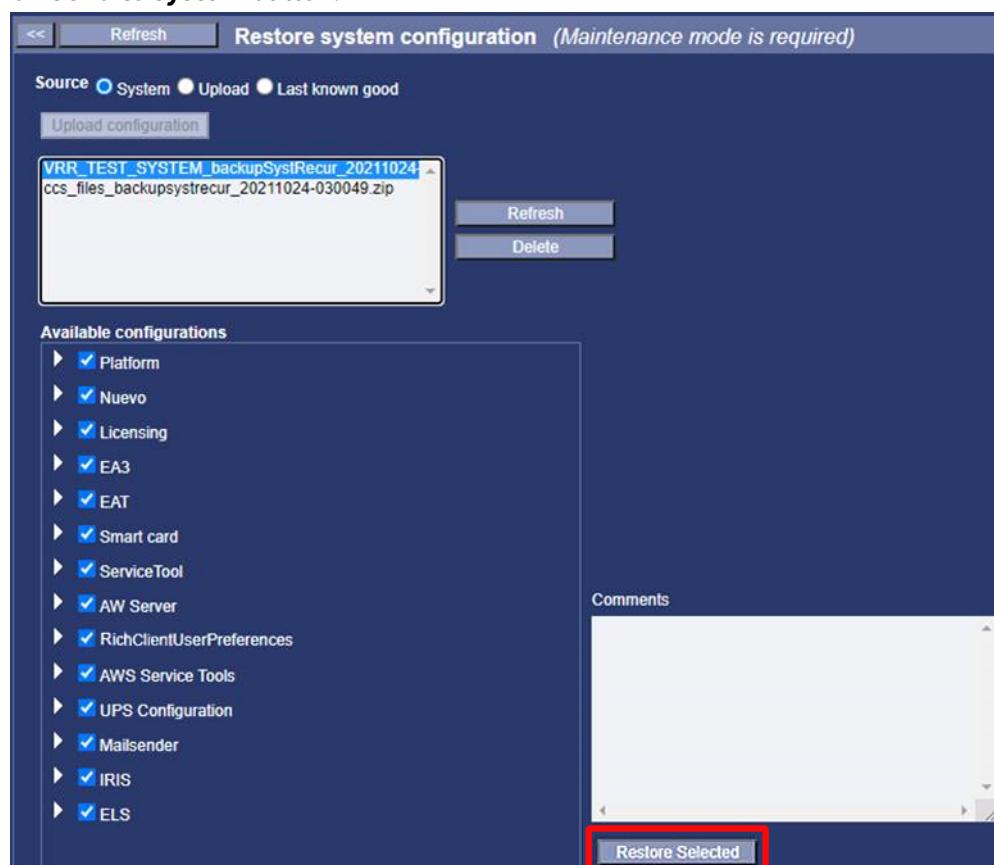
- c. For AW Servers with **Generic Hardening** active shall accept backups created in **Generic Hardening** systems or older configurations without any type of hardening.
  - d. For AW Servers with **Generic Hardening** active, backups created in **Secured for RMF** systems shall not be restored.
2. The AW Server is placed in Maintenance Mode. If not refer to [3.5 Entering the Maintenance Mode on page 486](#).
3. Click on **Maintenance/ Restore** to expand the menu then click on **System Configuration**.

#### **NOTE**

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. Click Refresh and a message in RED letters will display- The system is not in maintenance mode operation is not permitted

4. Select the **Source** for restoring:
- Check the **System** check box and select the file to restore.
  - OR
  - Check the **Upload** check box and click on **Upload configuration** button, to select the configuration file saved on an USB media or the Client PC.

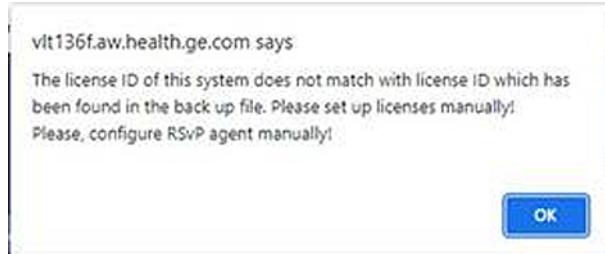
A popup window displays, click on the **Browse** button, choose the file to upload and click on **Send to system** button.



- If several configurations are stored on the server, or on your USB media or client PC, select the latest one if more recent and valid, or the "**Last known good**" configuration if you have previously selected it as reference backup.
5. Select the configuration to restore, then click on **Restore Selected** button.

6. The backup feature of AWS2.0 or AWS3.0 did not store the License ID. The restore feature of AW Server 3.2 is now doing a check on the License ID.

Therefore, when upgrading from a previous AWS2.0 or AWS3.0 release to AW Server 3.2, you will get the following warning message:



Click on **OK** button to accept.

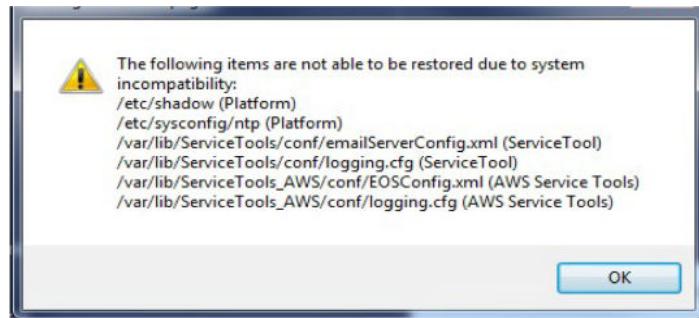
#### **NOTE**

If the license ID stored on the backup file is different from the License ID of the system you are reinstalling, the licenses will not be restored.

7. If the Imaging Cockpit components have been installed, a separate backup file, related to **CCS** check box, and containing the Imaging Cockpit configuration, has been created. To restore it, proceed as for a system configuration file. So, repeat [Step 4](#) and [Step 5](#) with the Imaging Cockpit configuration file.

8. **Parameters not restored**

- Passwords: All **passwords** are **restored to the default value**.
- Certain items cannot be restored due to incompatibility between the AWS2.0 / AWS3.0 platform and the AW Server 3.2 platform. Therefore you will get the following message to let you know that these items will not be restored.



- Click on **OK** button to accept.
- Click again on **Restore Selected** button.

A progress indication will display next to the “Restore selected” button, and then a GREEN successful indication if the restore was successful.

- The backup of an AW Server 3.2 Ext. 4.0 or Ext. 4.2 did not save the external CoLA server(s) IP address(es). Therefore, if the external CoLA server(s) IP address(es) were configured, they need to be added manually. Refer to [2.15.10.3 CoLA License server on page 157](#).
- The backup feature of **AW Server 2.0** or **AW Server 3.0** did not store the Hospital name and the backup recurrence parameters. Therefore they cannot be restored and shall be re-entered manually.

Another message may display at the end of the restore process, to let you know that the Integration configuration (if applicable) will not be restored:

*“The integration mode stored in the backup (seamless\_integ) has not been restored. Please configure it manually.”*

However, there is a "Prefill" utility allowing to populate the Integration fields with data that was saved, as part of the backup process. See next step.

## 9. Platform configuration:

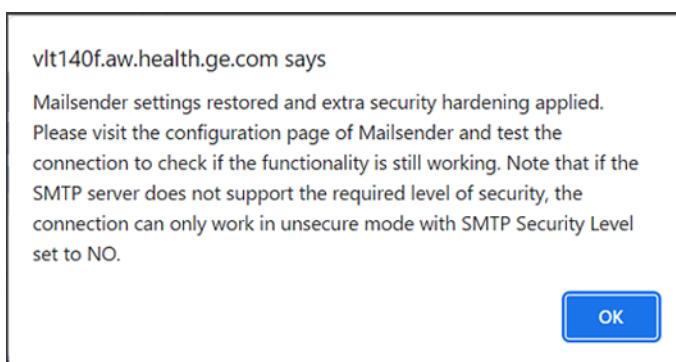
The Platform configuration has been restored, but needs to be applied to be effective.

- Click on **Initial Configuration/Platform Configuration**, check that the Platform license key displays, click **Next** to **Scalability** and check that the cluster mode is selected and HAPS server IP's are entered (if applicable), then click on **Next**, and use the **Prefill** button to populate **Integration** parameters (if applicable). Finally click on the **Apply** button.

Integration is addressed by [3.10.8 Integration restoration on page 532](#).

Scalability is addressed by [3.10.9 Scalability restoration on page 533](#) and [3.11.3 Software Upgrade within a Cluster on page 537](#).

- If the **Mailsender** check box is selected and the MailSender has been configured for secure (TLS) connection to the SMTP server, then the following warning message will appear:



The reason for the warning and the instruction to test the secure connection is, that AW Server will enforce TLS1.2 security protocol towards all external servers including the SMTP servers as earlier versions of TLS are not considered secure enough anymore. In earlier releases AW Server did allow also lower versions of TLS protocol (TLS1.1 and TLS1.0). In case the SMTP server does not support TLS1.2, then the secure connection which worked with earlier release will not work with this version of the AW Server. In this case the only way to make the connection work is to select **NO** for the **SMTP Security Level**.

## 11. Database Deletion Settings

Finally, make sure "Database Deletion Settings" have been properly restored, or proceed to setup (if applicable).

Refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#)  
**Informational step**

If the restoration takes much longer time and ends up with the message below, you may have done a mismatch between the network parameters you have entered through the tool, and those that you have just restored.



**DO NOT reboot your system at this time !!!!**

- Follow the steps "Repair the mismatched hostnames" described below.
  - Logout from the service tools session **or quit** the Internet Navigator

- Launch a new Internet navigator if necessary and http:// to the AW Server IP address
- Launch a new Service tools session and login as **service**.
- Go to **Maintenance** tab
- Go to **Network** sub-menu
- Click on the **Hostname** tab
- Modify the hostname so it reflects the DNS/Hostname (also AE Title) that your AW Server had before the upgrade.
- Click on **Apply** button.

The system will reboot

### 3.10.6.3 Licenses restoration

The licenses are restored during restoration of the configuration. However, the following steps should be performed in specific cases:

1. In case of **AW Server 2.0 release upgrade**: As it was not necessary to run the Volume Viewer basic application on AWS2.0, there was no license key for it. Therefore, the Volume Viewer license cannot not be restored. Refer to [2.15.10 Licensing Configuration on page 156](#) to license the applications.
2. In case of **AW Server 2.0 release upgrade**: Activate the applications since Applications are not activated by default, and if not activated, they would not be available on the Client. Refer to [2.17.4 Activate the Application\(s\) on page 181](#) to activate the applications.
3. Check that Pre-processing has been properly restored referring to [2.18.8 Preprocessing Configuration on page 204](#).

### 3.10.6.4 CardIQ Xpress Process (CXP) application reinstallation

It is possible to reinstall now from its own media or from the hard disk (if available), the CXP application, as the VV Apps have been reloaded and the license have been restored.

#### NOTE

There is an installation conflict between CardIQ Xpress Process and Advantage SIM MD. If Advantage SIM MD is installed on this AW Server, additional steps have to be performed:

1. Open a Terminal tool, login as **root**.
2. Uninstall Advantage SIM application using the following command:  
`/export/home/sdc/install/uninstall.advsim --complete <Enter>`
3. Install CardIQ Xpress Process application. Refer to [2.17.3 Install the Application\(s\) on page 178](#).
4. Install Advantage SIM application. Refer to [2.17.3 Install the Application\(s\) on page 178](#).

### 3.10.6.5 Internal Applications restoration

AW server software has some internal application: They are part of the AWS platform software and most of them will be restored part of the Backup/Restore process.

Verify that they have been properly restored.

- **Prodiag** - (Not applicable for Seamless integration and Secured for RMF mode) - Refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#)

- **SNMP traps** - (Not applicable in Secured for RMF mode) - Refer to [2.15 Job Card IST008 - Initial Configuration on page 140](#)
- **End Of Review** - Check that EOR has been properly restored or recreate it if it has not been restored. Refer to [2.18 Job Card IST010 - Administrative Configuration on page 184](#) for details.

## 3.10.7 RSvP connectivity re-installation

The Remote Connectivity has been restored (GEHC only). However, the RSvP Agent needs to be restarted.

1. From the Service Tools, select **Initial configuration > Remote Service > RSvP (GE Backoffice)**.



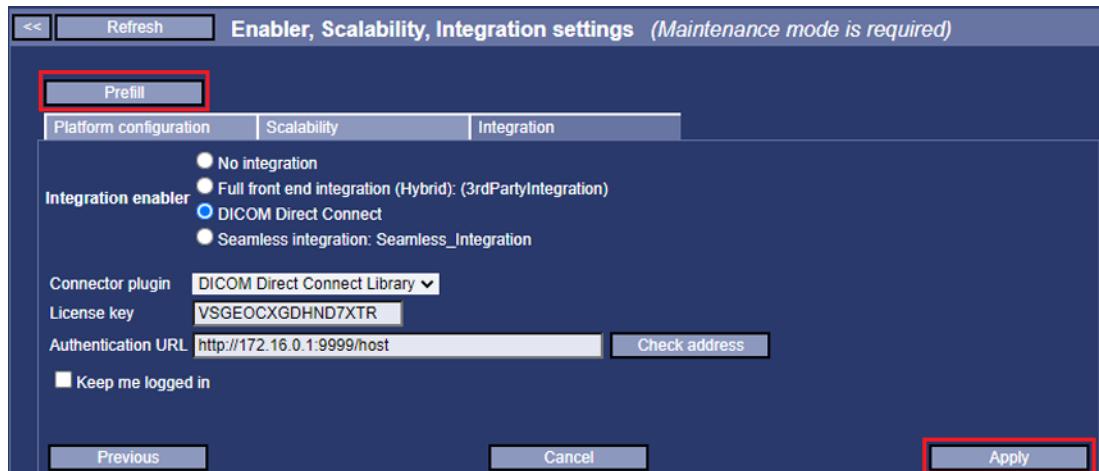
2. Click on the **Restart** button to restart the RSvP Agent.
3. Select the **Refresh** button to refresh the RSvP Agent status.

After some time the status turns green.

## 3.10.8 Integration restoration

The Platform configuration has been restored. However, it needs to be applied to be effective:

1. From the Service Tools, select **Initial configuration > Platform Configuration**.
2. Check that the **Platform license Key** displays.
3. Click on **Next** twice to display the **Integration** tab.



4. Click on the **Prefill** button to populate the integration parameters.

**NOTE**

If the integration parameters do not populate, enter them manually.

5. Click on **Apply** to apply the platform configuration.

Acknowledge the confirmation popups that display.

The AW Server reboot will be done later.

## 3.10.9 Scalability restoration

If applicable for your site, you shall restore the Scalability configuration.

- Perform the steps described in Chapter 2 [2.20 Job Card IST012 - Virtual Servers Cluster Configuration on page 244](#)

## 3.10.10 Security settings

### 3.10.10.1 System Hardening

Upon upgrade, the security Hardening needs to be reapplied to enforce the local user account password rules. Refer to [2.15.14 System Hardening on page 165](#).

### 3.10.10.2 Passwords restoration

Upon upgrade, passwords have been reset to the default values:

- Re-enter/change the passwords for your site (if applicable). Refer to [2.21 Job Card IST006 - Changing the Passwords on page 249](#).

## 3.10.11 Register System configuration

You shall now register the System configuration, in order to obtain the Activation key to unlock the AW Server. Perform the steps described in Chapter 2 [2.22 Job Card IST013 - System Configuration Registration on page 259](#) section 2.

**NOTICE**

Repeat this procedure after any intervention that changes the server's configuration, for instance when installing a new application or after an upgrade.

**Ensure you exit the Maintenance mode after System Registration. This will be done later in this procedure. Refer to [3.13 Exiting the Maintenance Mode on page 553](#).**

## 3.10.12 Upgrade AW Clients after AW Server Upgrade

In case of a simple software **re-installation** of AW Server, the Client re-installation/upgrade is not required. In case of an **upgrade** of AW Server, the Client upgrade is required.

- To upgrade the "**Standard**" AW Server client, perform the sections of chapter 2, [2.24 Job Card IST014A - Standard Client PC installation & Tests on page 270](#).

Standard stands for Standalone (no-integration) or any other modes of integration than the Seamless integration.

- To upgrade the "**Seamless**" AW Server client, perform the sections of chapter 2, [2.25 Job Card IST014B - Seamless Client PC installation and Tests on page 282](#).
- To upgrade the AW Server Web Client, perform the sections of [2.26 Job Card IST014C - Web Client Tests on page 286](#).

The first step consists on reconfiguring the Universal Viewer Server and the second step consists on upgrading a Client PC. Note that for seamless integration, the Universal Viewer Server must be reconfigured (see step 1 of the section / Job card referenced above).

## 3.10.13 Final tests and system handover to customer

### 3.10.13.1 Final settings and System handover to customer

- Perform the steps described in Chapter 2, [2.27 Job Card IST015 - Final Settings](#) on page 292
- Perform the steps described in Chapter 2, [2.28 Job Card IST016 - System Handover to Customer](#) on page 298.

#### NOTICE

If the AW Server you are upgrading has a large amount of patient data, image re-installation (database recovery) may not be complete before giving back the system to the user. **Warn the user that all patient data may not be available yet**, and that they shall preferably use the system for processing new exams, or be careful if they have to process existing exams.

### 3.10.13.2 GIB / SIEBEL update and paperwork

Send the customer's Global Installed Base data to GEHC. Send all paperwork from the installation to the appropriate recipient (i.e., GEHC or the customer).

Global Installed Base database may be directly updated using the following link:

EGIB @ <http://gib.gehealthcare.com>

- GEHC Global Install Base database web site is available from any outside web enabled PC.
- The FE can enter the model/serial into the Service Tools interface and send the GIB data up to GIB via email. So, make sure to fill-in all the information in the service tools Initial Configuration > Device Data & User Data.

#### NOTICE

USCAN System ID / Assets are no longer found in eGib and are now located in the CRM Siebel / Assets database.

- **"Installs:** Follow MyWorkshop document DOC1701877, Job Card IB Verification
- **"Upgrades:** Follow MyWorkshop document DOC1618060, Job Card FE Upgrade Instructions
- **"Asset Swaps:** Follow MyWorkshop document DOC1589267 Job Card FE Asset Swap

#### NOTE

EDS System remains on GIB until further notice.

#### NOTICE

Repeat this procedure after any intervention that changes the server's configuration, for instance installing a new application.

### 3.10.13.3 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.

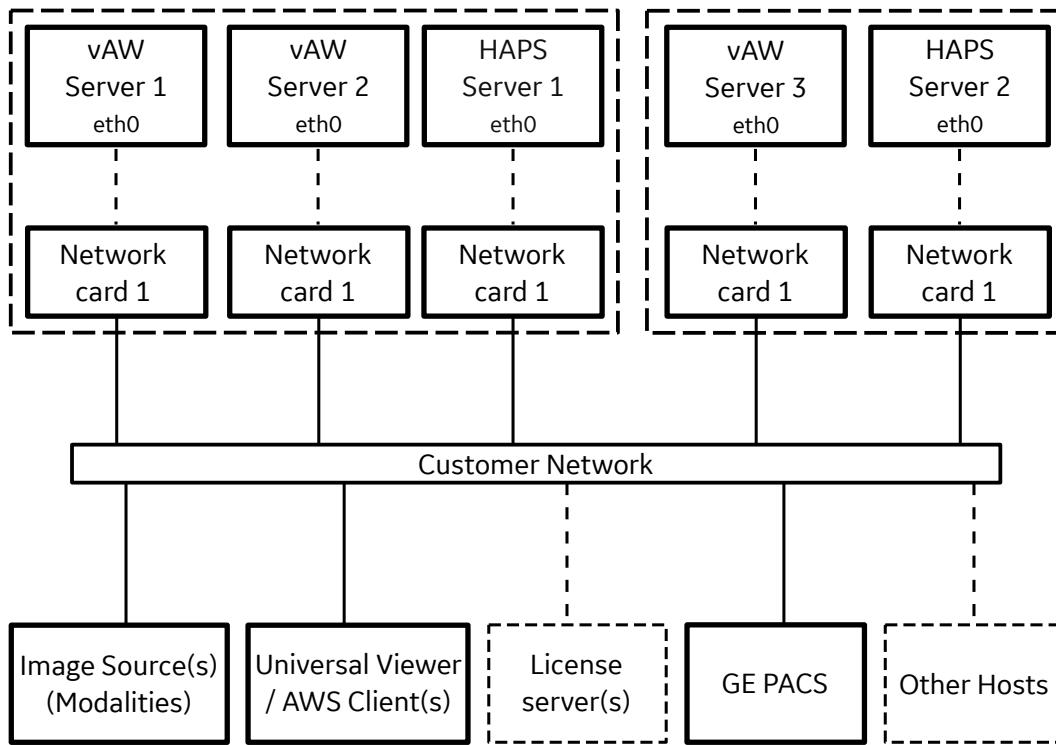
- Delete any corresponding ISO files that you may have stored on your GE laptop or other storage devices.
- Use the Version Management tool to Remove any old package from the Server.
- Retain installation media only for currently installed versions of software.
- Properly dispose of older installation media by destroying the media.
- If you need to reinstall an old version of software (perform a downgrade) at a later date on any given system you should re-order an up to date installation kit.

## 3.11 Job Card UPG002 - Scalability Upgrade

### 3.11.1 Adding an AW Server to an existing AW Servers Cluster

You have a cluster of AW Servers and you want to add a new AW Server to the cluster.

**Figure 3-8 Example of a new AW Server added to a cluster of 2 Virtual AW Servers**



It is possible to add a new AW Server node to an existing Cluster, in order to extend the number of concurrent users managed by the cluster. The new AW Server node can be installed on a new Hypervisor or on a Hypervisor that already hosts AW Server nodes.

The new node is installed by following the same steps as for the initial cluster installation. The only difference is that there is only one virtual AW Server to install.

To install a node, follow the workflow described in Section [2.4.3 Quick Start Installation Guide - Scalable Virtual servers on page 42](#).

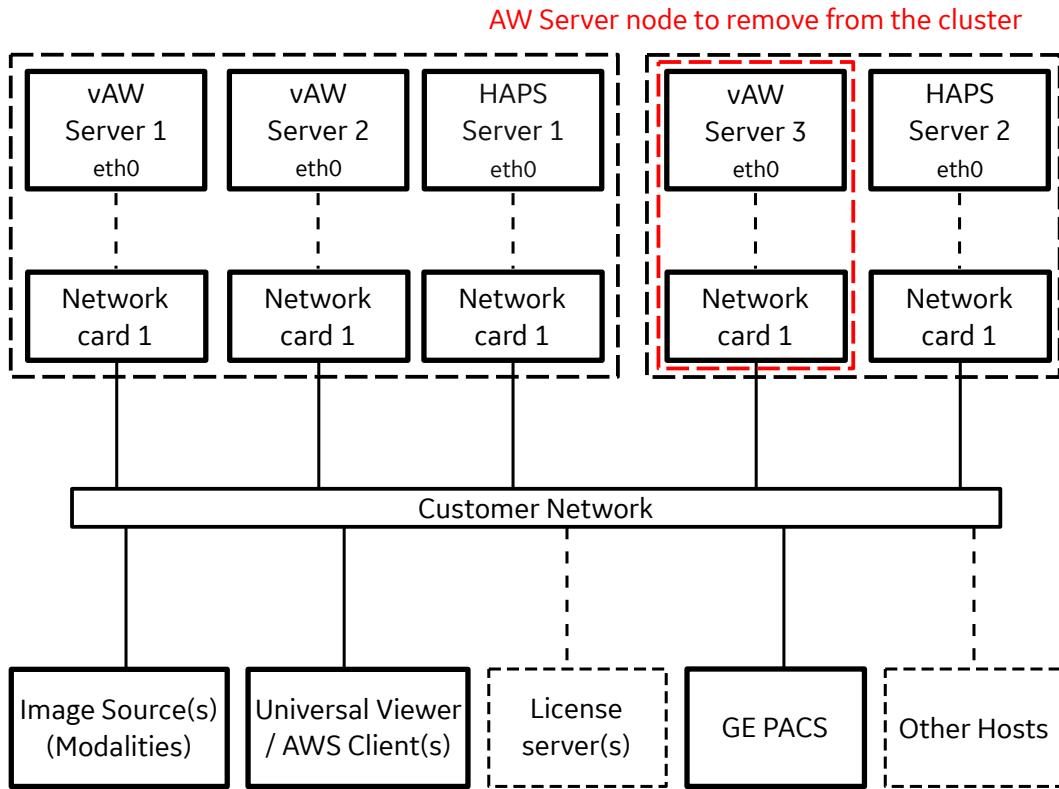
To summarize the installation steps:

- The **IT Admin** has to perform [2.7 Job Card IST001B - Virtual Machine creation](#) on page 68 to create the VM.
- The **GEHC FE** has to perform [2.9 Job Card IST002B - Virtual Machine Installation Verification](#) on page 87 to [2.22 Job Card IST013 - System Configuration Registration](#) on page 259, to setup the virtual AW Server.

## 3.11.2 Removing an AW Server from an AW Servers Cluster

To remove one AW Server from an AW Servers cluster, remove the AW Server node:

**Figure 3-9 Example of an AW Server removed from a cluster of 3 Virtual AW Servers**



1. Launch an Internet navigator and connect to the URL of the AW Server you want to remove.  
I.e: <http://3.24.45.12>.
2. Start the Service and Administrative Tools interface:
  - a. Click on the **Launch** button.
  - b. Login as **service**.
3. The AW Server is placed in Maintenance Mode. If not refer to [3.5 Entering the Maintenance Mode on page 486](#).

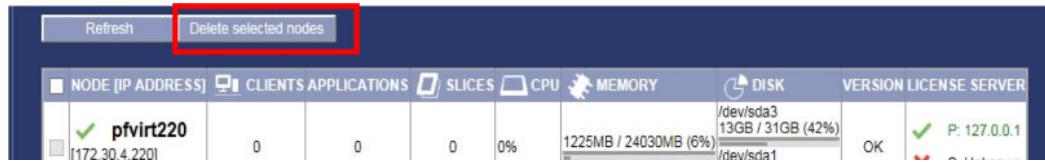
### NOTE

Only the users currently connected to the AW Server that is being removed will be disconnected. When they attempt to reconnect, they will be automatically redirected to one of the other AW Servers of the Cluster.

4. From the Service Tools, select **Initial Configuration > Scalability**.  
The *Manage and display scalability setting* interface appears.
5. Shutdown the AW Server.
6. Launch an Internet navigator and connect to the URL of one of the other AW Servers of the cluster.

I.e: <http://3.24.45.11>.

7. Start the Service and Administrative Tools interface, and login as **service**.
8. From the Service Tools, select **Initial Configuration > Scalability**.
9. Click on the radio button of the AW Server node to be removed, then click on **Delete selected nodes**.



10. Acknowledge the confirmation screen by clicking on **OK**.

The AW Server node is removed from the cluster.

### 3.11.3 Software Upgrade within a Cluster

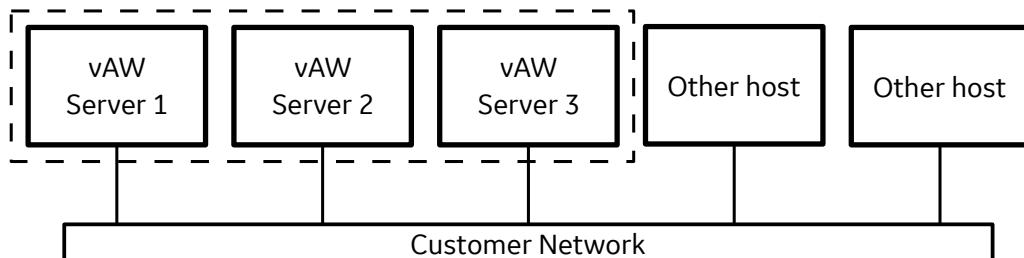
The following procedures are high level procedure, and refer to procedures already detailed in different sections of this manual.

#### 3.11.3.1 Pre-requisite for AW Server 3.0 upgrade case

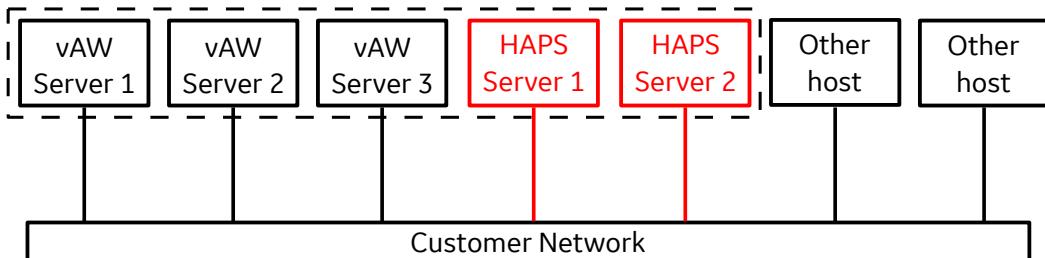
##### NOTICE

There is an important change for Preferences Sharing management brought by the AW Server 3.2 release. It is mandatory to **add two HAPS** (High Availability Preference Sharing) nodes to the cluster, prior to upgrade the AWS3.0 nodes to AWS3.2 nodes.

**Figure 3-10 Example of an AW Server 3.0 cluster before upgrade**



**Figure 3-11 Example of an AW Server 3.0 cluster during upgrade**



Two HAPS nodes must be created and added to the cluster before upgrading the AWS nodes.

- Refer to [2.8 Job Card IST001C - Virtual Servers Cluster Installation Steps on page 80](#) to create the HAPS virtual machine.
- Refer to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#) to create the HAPS server.

### 3.11.3.2 AW Server 3.0 High Level Upgrade Procedure

#### NOTICE

##### Prior to Software upgrade from AW Server 3.0 release case.

Make sure you have created/configured two new virtual machines for the HAPS (High Availability Preferences Sharing) servers. See [3.11.3.1 Pre-requisite for AW Server 3.0 upgrade case on page 537](#).

Three examples of high level upgrade are described in the following sections.

#### 3.11.3.2.1 Cluster of 2 Virtual AW Servers

You have a cluster of 2 AW Servers and you want to upgrade the software of the AW Servers and/or the Applications.

1. Place the AW Server 1 in Maintenance Mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

#### NOTE

Only the users currently connected to the AW Server that is being shutdown will be disconnected. When they reconnect, they will be redirected automatically to one of the other AW Servers of the Cluster. The IT admin of the site may want to warn the users of slightly degraded performances of the cluster, setting a Broadcast message from the operational AW Server.

2. Choose one of the following case:

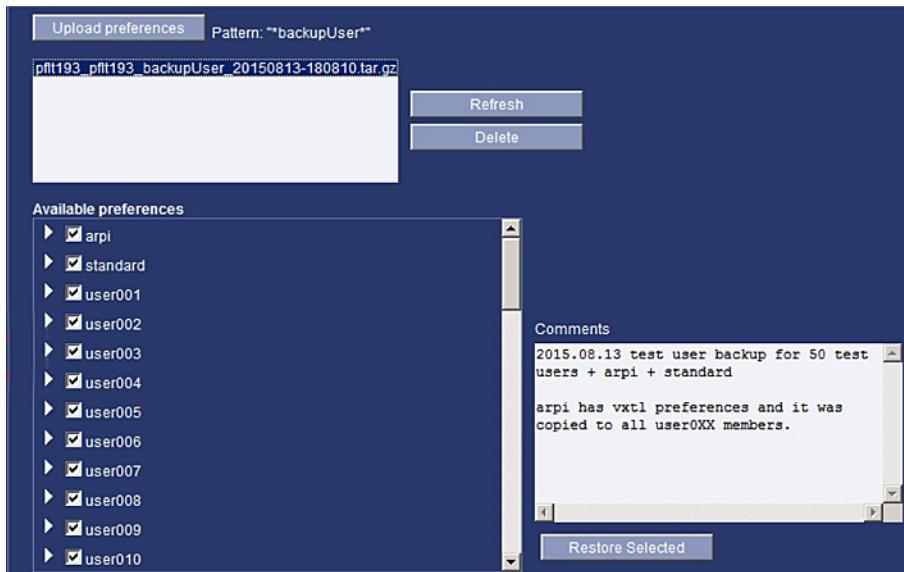
- If you want to upgrade applications only, refer to [2.1 Overview on page 29](#), [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#) for the applications upgrade procedure, then continue this procedure at [Step 8](#).
  - If you want to upgrade AWS platform, proceed to next steps. Refer to [3.10 Job Card UPG001 - Software Upgrade on page 495](#).
3. If you want a full software upgrade (Load From Cold - OS + AWS platform SW), first, save (write down) the Network parameters.
  4. Save the Site configuration - See section [3.10.3.3 Backup the Site configuration on page 503](#) for details.
  5. If you load from cold, reload the OS from the media.  
See section [3.10.4.3.2 Virtual AW Server on page 513](#) for details.

#### NOTICE

**DO NOT USE the OS OVF Template** for virtual AW which is for initial installation and creates at the same time the virtual machine.

6. If you want to load from cold, re-enter all network parameters.
7. Reload the AWS platform SW from the AW Server SW & Docs media.  
See section [3.10.4.4 AW Server Platform software installation on page 517](#) for details.
8. Reload the Applications from their respective media or upgraded Applications from the new media you have received.  
See section [3.10.5 Reload and reinstall the Advanced Applications on page 526](#) for details.
9. Reload the PACS integration plugin. Refer to section [2.19 Job Card IST011 - Integration on page 221](#) for details.

10. Restore the System configuration except for **RichClientUserPreferences**. Uncheck the **RichClientUserPreferences** checkbox before restoring.  
See section [3.10.6 Restore the Server configuration and licenses on page 527](#) for details on restore process.
11. Restore the Platform configuration, the Scalability configuration and the Integration configuration. Use the **Prefill** button to reload the Integration parameters.  
See section [3.10.6 Restore the Server configuration and licenses on page 527](#) for details on restore process.
12. When done with the Platform Configuration restoration, you will have to restore the User Preferences, as they now must be stored on the HAPS Servers. From the Service Tools menu, click on **Maintenance > Restore > User Preferences**.



13. Register the System configuration for the upgraded AW Server, and obtain a new Activation key, to exit the Maintenance mode.  
See section [3.10.11 Register System configuration on page 533](#) for details.
14. If it is an AW Server platform SW upgrade, the Client must be upgraded too. Proceed with one Client upgrade.  
See section [3.10.12 Upgrade AW Clients after AW Server Upgrade on page 533](#) for details.  
Note that this step would not be necessary if simply reloading the same SW release.
15. Shutdown the AW Server 1 and do not restart it yet!
16. When you are done with the upgrade of the AW Server 1, place the AW Server 2 in Maintenance (refer to [Step 1](#)).
17. Restart the AW Server 1. Make sure it is operational and that the integration mode is operational.
18. Set the Scalability mode on.
19. If AW Server platform SW upgrade, warn the IT admin of the site to proceed to the other Clients upgrade.

20. Proceed with the AW Server 2 upgrade, referring to previous steps, make sure Applications have been upgraded too (if applicable), that the PACS plugin has been reinstalled (if applicable), then put the Server back in the cluster when fully operational.

**NOTICE**

In the above and below mentioned cases, you shall register the new System configuration for each AW Server, and obtain a new Activation key, to exit the Maintenance mode.

### 3.11.3.2.2 Cluster of 3 Virtual AW Servers

You have a cluster of 3 AW Servers and you want to upgrade the software of the AW Servers and/or Applications.

The challenge is to keep 2 of the 3 AW Servers available as much as possible while doing the upgrade.

Referring to [3.11.3.2.1 Cluster of 2 Virtual AW Servers on page 538](#), proceed with the following high level sequence.

1. Place the AW Server 1 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
2. Upgrade the AW Server 1.
3. Restore the configuration and put the AW Server 1 back in operation.

**NOTE**

As the AW Server 1 does not have yet the Golden set, it will not be accessible to the users yet.

4. Place the AW Server 2 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
5. Upgrade the AW Server 2.
6. Restore the configuration and put AW Server 2 back in operation.

The AW Server 1 and AW Server 2 are now upgraded to the new version. They are ready to takeover and AW Server 3 can be disconnected now.

7. Place the AW Server 3 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

All Clients will be disconnected for a while, time to set the Golden set on the newly upgraded AW Server 1 and AW Server 2.

8. Set the Golden set for AW Server 1 or AW Server 2.

Now the AW Server 1 and AW Server 2 are taking over. Clients can reconnect.

9. Upgrade the AW Server 3.

10. Restore the configuration, set the Golden set and put the AW Server 3 back in operation.

### 3.11.3.2.3 Cluster of 4 Virtual AW Servers

You have a cluster of 4 AW Servers and you want to upgrade the software of the AW Servers and/or Applications. Referring to [3.11.3.2.1 Cluster of 2 Virtual AW Servers on page 538](#), proceed with the following high level sequence.

1. Place the AW Server 1 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
2. Upgrade the AW Server 1.

3. Restore the configuration and put the AW Server 1 back in operation.

**NOTE**

As the AW Server 1 does not have yet the Golden set, it will not be accessible to the users yet.

4. Place the AW Server 2 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

5. Upgrade the AW Server 2.

6. Restore the configuration and put AW Server 2 back in operation.

AW Server 1 and AW Server 2 are now upgraded to the new version. They are ready to take over and AW Server 3 can be disconnected now.

7. Place the AW Server 3 and AW Server 4 in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).

All Clients will be disconnected for a while, time to set the Golden set on the newly upgraded AW Server 1 and AW Server 2.

8. Set the Golden set for the AW Server 1 or AW Server 2.

Now the AW Server 1 and AW Server 2 are taking over. Clients can reconnect.

9. Upgrade the AW Server 3 and AW Server 4.

10. Restore the configuration, set the Golden set and put the AW Server 3 and AW Server 4 back in operation.

### 3.11.3.3 AW Server 3.2 High Level Upgrade Procedure

When upgrading a cluster of AW Server 3.2 to the latest release, it is necessary to upgrade each AW server within the cluster, as well of upgrading the two HAPS (High Availability Preference) servers.

#### 3.11.3.3.1 Upgrade case 1

The customer agrees that all the AW Servers within the cluster will be unavailable to the users, and can be placed in maintenance mode during the time necessary to upgrade the AW Servers and the HAPS servers.

1. Backup the system configuration:

- a. Place all AW Servers in Maintenance mode. Refer to [3.5 Entering the Maintenance Mode on page 486](#).
- b. Proceed to the upgrade of the system configuration (including preferences) for each AW Server.

2. Upgrade the HAPS servers:

- a. Proceed to the upgrade of the OS and AWS platform software for the two HAPS VMs. DO NOT use the OVF Template media for OS upgrade, but use the OS for VM media. Refer to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#) to load the AWS / HAPS platform software.

- b. Select **HA Filesystem server**.

3. Upgrade the AW servers:

- a. Proceed to the upgrade of the OS, AWS platform software, and Applications for each of the AW Server VMs and install the Dakota client for Seamless integration.
- b. DO NOT use the OVF Template media for OS upgrade, but use the OS for VM media. Refer to [2.11 Job Card IST003 - Installation of Platform Software on page 109](#) to load the AWS / HAPS platform software. Select **AW server**.

- c. Restore the configuration (including Preferences) for each AW Server.
  - d. Setup the Golden Set.
  - e. Register the configuration for all servers then quit the maintenance mode.
4. Upgrade the AW server Clients: Proceed to the upgrade of the AW Server Client software.

### 3.11.3.3.2 Upgrade case 2

#### NOTICE

**This procedure requires that two new HAPS servers are created, so that the Preferences can be copied to those new servers. When done, the old HAPS servers will be deleted.**

The customer request that as many AW Servers as possible are left up and running as long as possible, during the whole time necessary to upgrade the AW Servers and the HAPS servers.

Example: Cluster of 3 virtual AW Servers

Below is the example of a 3 nodes cluster AW Server 3.2 with 2 HAPS nodes, to be upgraded to the latest AW Server 3.2 release.

1. Create two new HAPS servers:

- a. Ask the IT administrator of the site to create two new virtual machines from the new OVF Template OS in order to host the two new HAPS servers.

For these new HAPS servers, two new IP addresses on the Hospital network are needed (IT Admin responsibility).

#### NOTE

In order to achieve high availability of the Preferences, the two HAPS servers shall preferably be hosted on two different Hypervisors. Refer to [2.7 Job Card IST001B - Virtual Machine creation on page 68](#) for VM creation instructions.

- b. When done with the VM creation, proceed to steps described in [2.11 Job Card IST003 - Installation of Platform Software on page 109](#) to load the AWS / HAPS platform software.
  - c. Select **HA Filesystem server**.
2. Upgrade the AW Server 1:
    - a. Shutdown the AW Server 1.
    - b. Install new OS release (do not use the OVF template, but use the new OS for VM), the new AWS release, the up to date Dakota client (for Seamless integration), and applications and the licenses.
    - c. Configure the server in cluster mode.
    - d. Connect to the new HAPS nodes.
  - The AW Server 1 is out of the cluster, the AW Server 2 and AW Server 3 are still in the cluster and can be used by the radiologists.
    3. Upgrade the AW Server 2:
      - a. Inform users to save all new preferences.
      - b. Create a preferences backup.
      - c. Shutdown the AW Server 2.
      - d. Install the new OS, AWS version, Dakota client (for Seamless integration), applications and licenses (keep backup partition or save backup file to any removable media).
      - e. Configure the server in cluster mode.

- f. Connect to new HAPS nodes.
- g. Restore the preferences backup on the AW Server 2.
- h. Verify that all preferences were restored properly.

After the installation of the AW Server 2, only the AW Server 3 is available to the users.

4. Finish the maintenance of the AW Server 1 and AW Server 2, and set a new Golden set to one of these AW Server.

As the Golden set is selected, the AW Server 1 and AW Server 2 become available to the users. Users on the AW Server 3 are warned to save their work, exit then log in again.

#### **NOTE**

Users shall upgrade AWS client before the new login.

5. Upgrade the AW Server 3:

- a. Shutdown the AW Server 3.
- b. Install the new OS, AWS version, Dakota client (for Seamless integration), applications and licenses.
- c. Configure the server in cluster mode.
- d. Connect to new HAPS nodes.

After the installation of the AW Server 3, the whole cluster is up and running.

6. Shut down the old AWS 3.2 HAPS nodes and delete them.

7. Notify the IT admin of the site that the IP addresses of the old HAPS servers are no longer needed.

8. Upgrade the AWS Clients.

9. Notify the IT admin of the site to make sure that all the AWS Clients have been upgraded to the new AWS 3.2 release.

## **3.12 Job Card UPG003 - Hardware Upgrade**

### **3.12.1 Foreword**

This section outlines the various steps necessary to upgrade an older AW Server hardware to the latest AW Server hardware. The hardware upgrade offerings currently consist on a complete hardware swap.

The upgrade steps are summarized hereafter:

- Install your new AWS system following instructions given at [2.1 Overview on page 29](#).

Preferably use the IP address of the old AW Server for the new server (you will not have to change the settings on the other DICOM hosts), making sure that the old server is disconnected from the network or that you have changed its IP address to a temporary one, if you need to transfer image data from old to new server.

- Contact your On-Line Support so that the licenses available on the old AW Server are transferred (adapted) to the License ID of the new AW Server.
- Perform a quick check on the old hardware
- Save the system configuration of the old hardware
- Check with the customer IT admin if the patient data is already stored on another system (PACS for instance) and can be deleted from the older system.

- Optional step: If patient data shall be transferred to the new hardware:
  - Warn the IT admin that this operation may take several hours depending on the number of images/patients data to be transferred.
  - Check with IT admin how much patient data shall be reinstalled, and how much data can be deleted in order to save time.
  - Ask the IT admin for a temporary IP address to be used for the older AW server, time to transfer the patient data.
  - Make sure clients are no longer connected on the older AW server
  - Change the IP address of the older server to the temporary IP address.
  - Proceed with image data transfer from older AW server to new AW Server
  - Declare the images/patients into the new AW server database.
- When done, proceed with image data deletion of the older AW server
- Proceed with disassembly and packaging of the older server, using the packaging of the new server
- Proceed with old server shipment to recycling center

### 3.12.2 Old hardware checks

- Proceed with old hardware checks referring to [3.10.2 Verify that AW Server is operational on page 498](#).

### 3.12.3 Old hardware configuration backup

- Login to the Service Tools interface.
- The AW Server is placed in Maintenance Mode. If not refer to [3.5 Entering the Maintenance Mode on page 486](#).
- Proceed with old hardware configuration backup referring to [3.10.3 Backup the configuration on page 500](#).

### 3.12.4 New hardware installation - High level steps

New AWS hardware or new AWS Virtual hardware installation must be complete prior to perform the following steps, and it is necessary that the minimum configuration steps have been completed.

Make sure the new hardware or Virtual hardware installation and minimum necessary configuration are complete, referring to instructions given at chapter 2 and summarized hereafter:

Install the AW Server 3.2 hardware server or AW Server 3.2 Virtual server

1. Configure the Network parameters
2. Configure Date & Time parameters
3. Load the Applications from media (Virtual AW Server case)
4. Restore the old AWS2.0 hardware configuration to the new AWS3.2 hardware except for:
  - GIB - Uncheck box in Restore Config menu
  - Device Data - Uncheck box in Restore Config menu
  - Other non-applicable parameters such as licenses are automatically not restored.

(See next section for details)

5. Configure the rest of the new AW Server 3.2 parameters
  - Licenses
  - GIB
  - Device Data
  - Remote access
  - Registration Key
6. Upgrade the AWS Client
7. Proceed to final settings and system handover to customer.

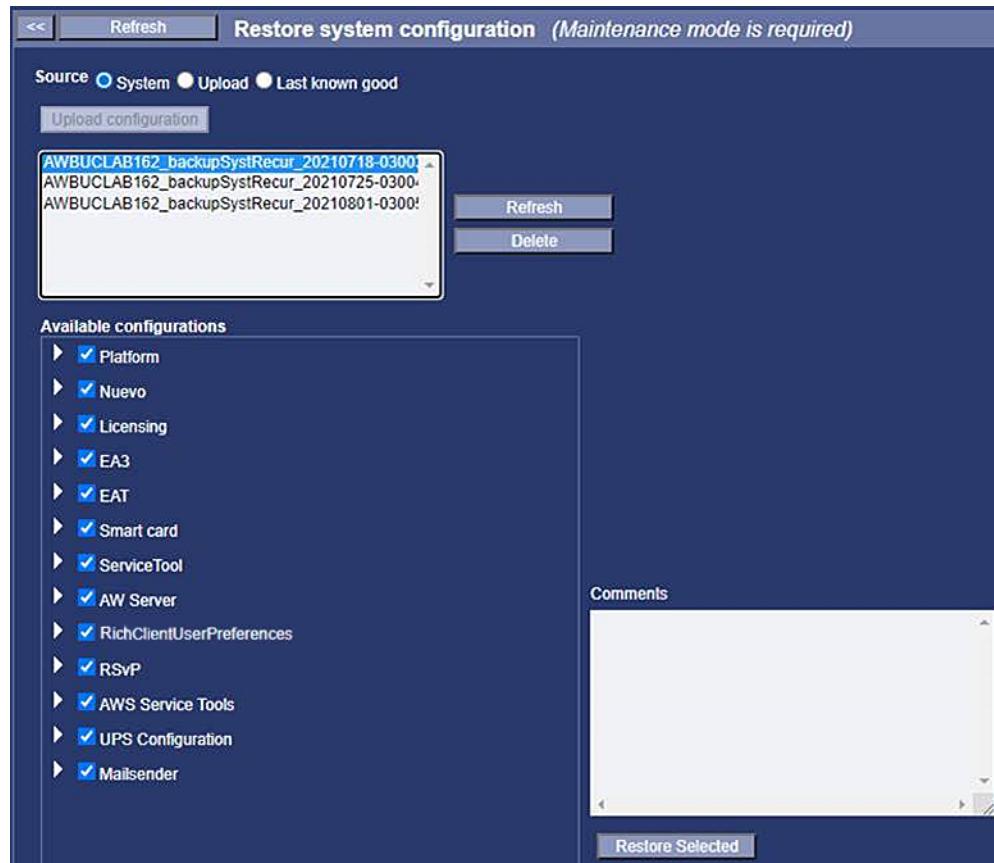
### 3.12.5 System Configuration restoration

You may now want to restore some items of the old AW Server System configuration such as remote hosts to the new AW Server.

However not all of the configuration can be restored.

Make sure to un-check at least the Nuevo, Licensing and RSvP check boxes that are specific to the old server, before restoring the old to new AW Server configuration.

Refer to [3.10.6 Restore the Server configuration and licenses on page 527](#) for details on the restore process.



### 3.12.6 Patient data transfer

The currently stored image data can be transferred from the old hardware to the virtual AW Server, if that is requested by the customer. Warn the customer that this process may take a long time depending on the number of images to be transferred.

## NOTICE

When image transfer is requested by the user, in order to save time (I.e: High Tier server image filesystem size is 4TB to 6TB), and limit the impact on the new AW Server (I.e: Virtual AW Server max disk size is 6TB), a choice should be made in advance by the customer on what image data must be kept and what image data can be erased.

- Make sure with the customer or IT Admin about what image data can be erased.
- Proceed with all possible image data deletion, prior to transfer image data from old hardware server to new AW server. The currently supported maximum disk size for AW Server (physical or virtual) image filesystem is 6TB.

## NOTICE

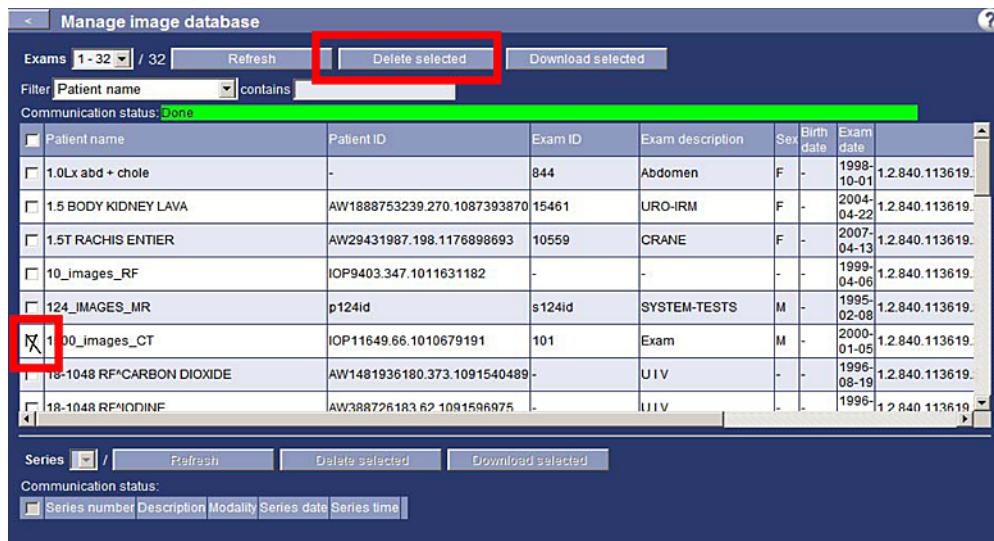
The following should NOT be considered as a standard procedure, as the time necessary to transfer the images may greatly affect the installation / upgrade time. Make sure this extra time has been planned in the overall installation time.

### 3.12.6.1 Check with customer what images can be deleted and proceed to deletion

If it is possible to delete some of the patient data contained into the AW Server database, because this data is already saved in the PACS, or still contained into the Image source database, it will save transfer time and then re-installation time.

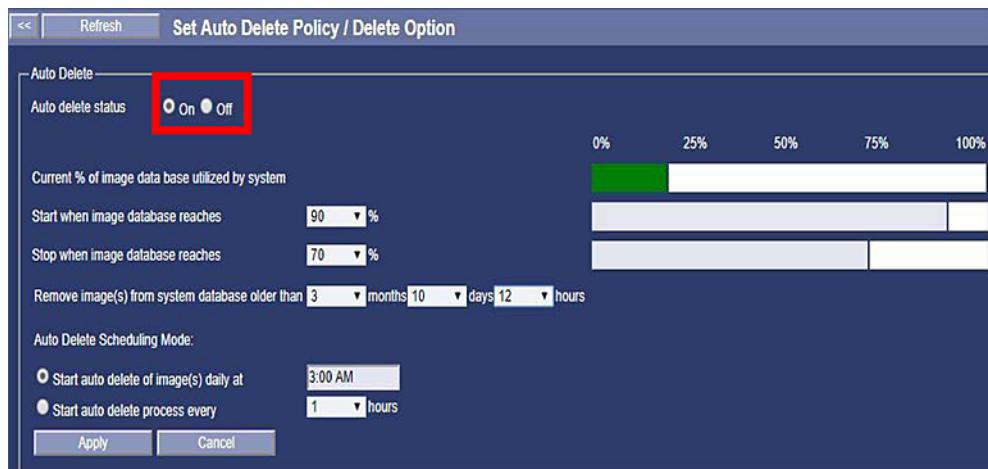
To delete images at the old AW server, proceed as follows:

- Login to the old AW Server Service Tools interface and select **Administrative / Utilities / Image Database**
- Select patient exams candidate for deletion
- Click on **Delete selected** button, and acknowledge the confirmation message:



### 3.12.6.2 De-activation of Auto-delete on the old AW Server

- From the Service Tools **Initial Configuration / Auto-delete**, de-activate Auto Delete (if applicable).
- Click on **Apply** to save.



When done with image deletion and de-activation of Auto-delete, proceed with IP address change so that the old server and new server can be placed on the same network.

### 3.12.6.3 Change the IP address of the older AW server

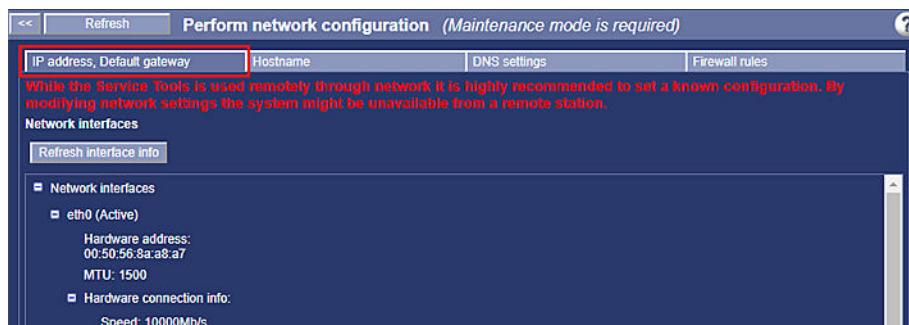
You will use the old server IP address for the new AW server

You will give a temporary IP address (in the same sub-network) to the old server.

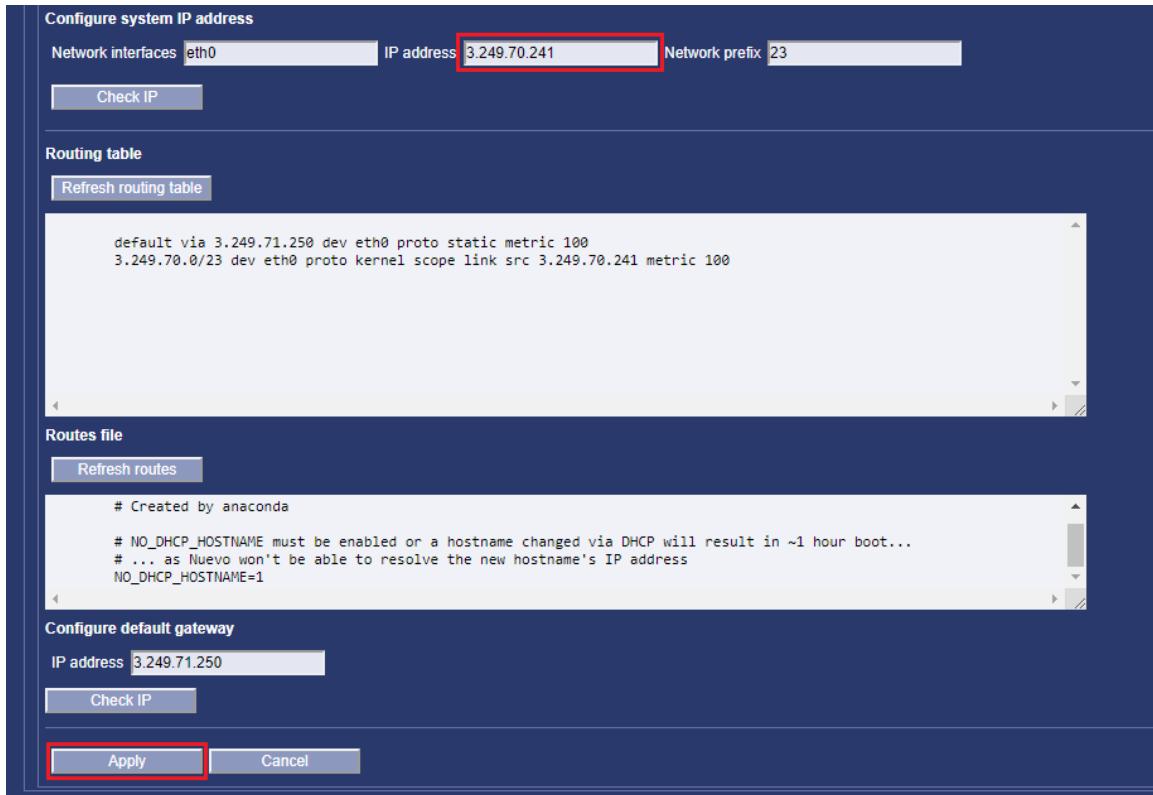
#### **NOTICE**

If the new AW server is not in the same sub-network as the old server, you cannot give the old server IP address to the new server. Keep the IP addresses as they are, then you will declare the IP address of the new server to the DICOM hosts on your network, to ensure the DICOM transfers.

1. Login to the Service Tools interface.
2. The AW Server is placed in Maintenance Mode. If not refer to [3.5 Entering the Maintenance Mode on page 486](#).
3. Click on **Maintenance / Network**



4. Click on **IP address, Default gateway** tab
5. Change the IP address to the temporary address.



6. Click on **Apply** and accept the reboot of the server.
7. When the old server has rebooted, make sure it is visible (can be ping'ed) on the network with its new temporary address.

### 3.12.6.4 Prepare the old AW Server for image transfer

**The following shall be done at the OLD AW Server.**

- Open a Terminal tool on the old AW Server from the Service Tools interface
- Log as **root**.
- De-activate the Firewall on the old AW Server. In the Terminal, type:  
**systemctl stop pnf <Enter>**
- Enable ssh - In the Terminal, type:  
**ssh\_enabler <Enter>**

### 3.12.6.5 Image transfer from old to new AW Server

**The following shall be done at the NEW AW Server.**

- Open the KVM or open a Terminal tool from the Service Tools interface.
- Log as **root**.
- Switch user to "sdc"
- Launch the image transfer script  
**su - sdc <Enter>**
- Launch the image transfer script

**/usr/share/ServiceTools\_AWS/scripts/db\_transfer/pull\_images <IP\_address\_old\_server> <Enter>**

I.e: /usr/share/ServiceTools\_AWS/scripts/db\_transfer/pull\_images 3.249.12.68 <Enter>

Lots of output will display such as:

*Could not open a connection to your authentication agent.*

#####

*Check dirs and files having been defined in a setVariables file on the local host*

*SCRIPTONREMOTE=/usr/share/ServiceTools\_AWS/scripts/db\_transfer/runOnRemoteSite.sh*

.....

*Check the system AWS or AW AWS*

#####

*Remote RUN script originality check*

.....

*Remote host ping test*

*Host is OK*

#####

*Remote host port (22) check*

*Connection to 3.249.12.68 22 port [tcp/ssh] succeeded!*

*Port (22) is OK (open)*

#####

*Prepare the automatic log in*

*Check the .ssh dir*

#####

.....

#####

*Log in to Remote host*

*Could not open a connection to your authentication agent.*

### **WARNING**



*Permanently added '3.249.12.68' (RSA) to the list of known hosts.*

*root@3.249.12.68's password:*

- Enter the OLD SERVER root password and press <Enter>

*More output will display such as:*

#####

*Check the remote directory (/export/home1/sdc\_image\_pool/images/)*

#####

*Calculating required and available spaces ...*

#####

*Run rsync*

*[=====]*

*100%#####*

**NOTE**

Time necessary to complete the transfer images (100%) will depend on the number of images to be transferred and the speed of Network at your site.

*Set back.sh files on remote host*

```
#####
#
```

*Set back the .ssh files on local host*

```
#####
#
```

Then images are declared (installed) on the new AW Server

*Declare images on the host*

*/export/home/sdc/nuevo/bin/dbExpressInstall*

*Using log name = default, logging to /export/home/sdc/nuevo/logfiles/terra.log*

*Using log name = /export/home/sdc/logfiles/db\_transfer.log, logging to /export/home/sdc/logfiles/db\_transfer.log*

*Amount of disk space to be reserved: 311715956*

*The configuration file is ::/export/home/sdc/terra/resources/terra.cfg*

*ER\_EVENT\_TIMEDOUT is :: 0*

**NOTE**

If some errors occur while declaring the images (most of the time when the image is already stored on the new server - demo images for example), you will get the following kind of message:

*Installing ... One or more file could not be declared !!! Please check the logfile: /export/home/sdc/logfiles/db\_transfer.log. Declaration has been done with ERROR*

- Check what exams were not properly transferred and warn the IT admin of the site, so that they can check the reason in case some exams were not properly copied, and make sure they could solve the issue before you erase the exam(s) from the old server.

You can also check the **/export/home/sdc/logfiles/db\_transfer.log** logfile for errors, then check the corresponding exam(s) integrity as shown in next section.

- After having analyzed the **db\_transfer.log** logfile, delete it in order to save disk space:

**rm /export/home/sdc/logfiles/db\_transfer.log <Enter>**

### 3.12.6.6 Check installation of images on the new AW Server

- Login to the new AW Server Service Tools interface and select **Administrative > Utilities > Image Database**.
- Check that all exams have been properly re-installed in the new AW Server.
  - Select / highlight each Patient name and check that the number of series is consistent
  - Select highlight each Series and check that the number of Images is consistent.

The screenshot shows a software interface for managing medical image data. At the top, there is a table listing patients with their names, acquisition dates, and other relevant information. Below this, there are two sections for 'Series' and 'Images', each with a list of items and corresponding download buttons. A green progress bar at the bottom of each section indicates the status of the operations.

|                                     | BONE , Deluxe   | 01-15-68 | 17310 | RIGHT KNEE | M | - | 1990-09-27 | S. BARAD, M.D.   | MR | 1.2.840.113619.2.1.1.2703349038.985  |
|-------------------------------------|-----------------|----------|-------|------------|---|---|------------|------------------|----|--------------------------------------|
| <input type="checkbox"/>            | BRAIN_MR        | 0720494  | 8236  | BRAIN      | F | - | 1994-01-10 | DR.GANS          | MR | 1.2.840.113619.2.1.1.322987149.467.7 |
| <input type="checkbox"/>            | COTES , Debourg | 3-16-63  | 17611 | BRAIN      | M | - | 1996-10-22 | J. STOODY M.D.   | MR | 1.2.840.113619.2.1.1.2703349038.113  |
| <input checked="" type="checkbox"/> | DOG , Hot       | 03-18-52 | 17741 | L-SPINE    | M | - | 1996-10-31 | H. KHASIGIAN, MD | MR | 1.2.840.113619.2.1.1.2703349038.470  |

| Series                              | 1 - 5         | / 5                     | Refresh  | Delete selected | Download selected |                                                   |
|-------------------------------------|---------------|-------------------------|----------|-----------------|-------------------|---------------------------------------------------|
| Communication status: Done          |               |                         |          |                 |                   |                                                   |
| <input type="checkbox"/>            | Series number | Description             | Modality | Series date     | Series time       | Instance unique identifier                        |
| <input type="checkbox"/>            | 2             | T2 FSE SAGITTAL SERIES  | MR       | 1996-10-31      | 15:12:39          | 1.2.840.113619.2.1.1.2703349038.470.846689869.999 |
| <input type="checkbox"/>            | 1             | SAGITTAL LOCALIZER      | MR       | 1996-10-31      | 15:08:05          | 1.2.840.113619.2.1.1.2703349038.470.846689869.989 |
| <input type="checkbox"/>            | 4             | T1 AXIAL OBLIQUE SERIES | MR       | 1996-10-31      | 15:24:03          | 1.2.840.113619.2.1.1.2703349038.470.846689870.25  |
| <input type="checkbox"/>            | 3             | T1 SAGITTAL SERIES      | MR       | 1996-10-31      | 15:18:59          | 1.2.840.113619.2.1.1.2703349038.470.846689870.13  |
| <input checked="" type="checkbox"/> | 5             | T2 FSE AXIAL SERIES     | MR       | 1996-10-31      | 15:32:02          | 1.2.840.113619.2.1.1.2703349038.470.846689870.42  |

| Images                         | 1 - 30           | / 30             | Refresh            | Download selected | Dump header                                      |
|--------------------------------|------------------|------------------|--------------------|-------------------|--------------------------------------------------|
| Path: p12/e12/s43/2786.MRDC.13 |                  |                  |                    |                   |                                                  |
| Communication status: Done     |                  |                  |                    |                   |                                                  |
| <input type="checkbox"/>       | Acquisition date | Acquisition time | Acquisition number | Instance number   | Instance unique identifier                       |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:03         | 1                  | 1                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.43 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 2                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.44 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 3                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.45 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 4                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.46 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 5                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.47 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 6                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.48 |
| <input type="checkbox"/>       | 1996-10-31       | 15:32:06         | 1                  | 7                 | 1.2.840.113619.2.1.1.2703349038.470.846689870.49 |

### 3.12.6.7 Final steps on the new AW Server

#### NOTICE

When transferring image data from the old to new AW Server, "locked" exams may have been reset to "unlocked". Warn the customer / IT Admin that they will have to reset the "lock" on those exams, through the AW Server Client UI.

### 3.12.6.8 Final steps on the old AW Server - Delete Patient data

#### NOTICE

**NEVER SEND BACK an old system containing Patient data.** Systematically proceed to complete patient data deletion on the old AW Server, and "wipe out" hard disks before returning hardware to the recycling center.

Before proceeding with file deletion of your old hardware, make sure that you have saved all necessary files to install the new hardware. Also make sure that the customers have saved their own files.

#### NOTICE

The procedure can take a long time, depending on the number of images stored on the image disks.

**NOTE**

The below procedures are the responsibility of GEHC for the physical AW servers. For virtual AW Server, it is the Customer's responsibility to perform the wiping of their hypervisor Storage media.

To be compliant, you must use one of the following tools to perform a complete secure wiping of Customer System Storage media:

- **Blancco Drive Eraser**

This is the recommended tool as it does not rely on tool shipment/availability and does not require disassembly and removal of hard drives from equipment.

This is a 3rd party disk erasure software that may be downloaded from a secure GE shared storage location at any time by authorized personnel. Technicians will be able to create local boot images for secure wipes of the imaging equipment as needed.

After inserting in the workstation the bootable media (DVD/USB) containing the software, the workstation will boot on it and the Blancco software will allow you to erase all the disks.

- **Disk management Tool**

You must order it from the Service Tools Pool, then remove the disks from the workstation and connect them to the Disk Management Tool to erase them.

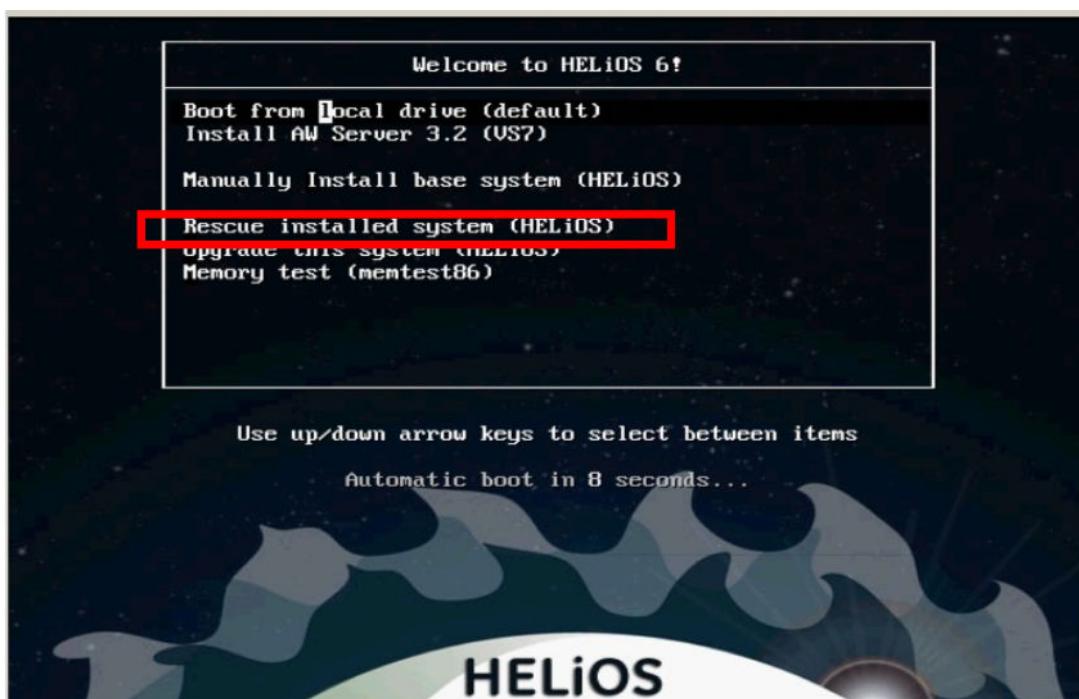
Follow instructions given in the 5500610-1EN - Disk Management Tool Service Manual delivered within the kit.

- Refer to Service Note SNAW3037 - Secure Wipes of Customer System Storage Media (DOC1615300) for the detailed procedure to erase patient data.

OR

- If any of the above tool are available, use the procedure described hereafter:

1. Insert the new AW Server 3.2 OS DVD into the old server's DVD drive.
2. Reboot the old AW server
3. When the DVD's boot menu displays, arrow down to select the option: **Rescue installed system.**



Boot messages display, then a few screens will pop up:

4. Page through the rescue options to launch a command shell:
  - Choose Language: >>> select **English**
  - Keyboard type: >>> select **US**
  - Setup Networking: >>> select **No** at the question "Do you want to start the Network interfaces ..."
  - Rescue: >>>> tab to select **Skip** at the messages "The rescue environment will now ...."
  - Shell: Start shell >>> tab to select **OK**

You will now get access to the system via the Command prompt

5. SUN or HP server: Type the following commands:

**ls /dev/sd\* <Enter>**

Normally, if all disks are present and still functional, you will see the partitions /dev/sda, and /dev/sdb which correspond to the system partition and the images partition. Note that you will also see the sub-partitions of sda and sdb such as sda1, sda2, sda3, sdb1, sdb2.

**parted /dev/sda print <Enter>**

**parted /dev/sdb print <Enter>**

- Then type in:

**dd if=/dev/zero of=/dev/sda & <Enter>**

**dd if=/dev/zero of=/dev/sdb & <Enter>**

- Wait for at least 20 minutes, then ensure that the partitions are no more readable

parted /dev/sda print <Enter> shall indicate that the disk label is not recognized

parted /dev/sdb print <Enter> shall indicate that the disk label is not recognized

6. Eject the OS DVD

7. Halt the server

**halt <Enter>**

8. Power off the server

When the System is "halted", power off the server.

### 3.12.7 Old hardware return procedure

Old hardware equipment shall be returned to the **GEHC Recycling Centers**.

Ask your Support Center for the appropriate procedure for your region.

Use the shipping boxes of your new hardware to pack the parts you are returning.

Refer to Chapter 5, [A.10 Hardware Return Procedure on page 599](#) for instructions

## 3.13 Exiting the Maintenance Mode

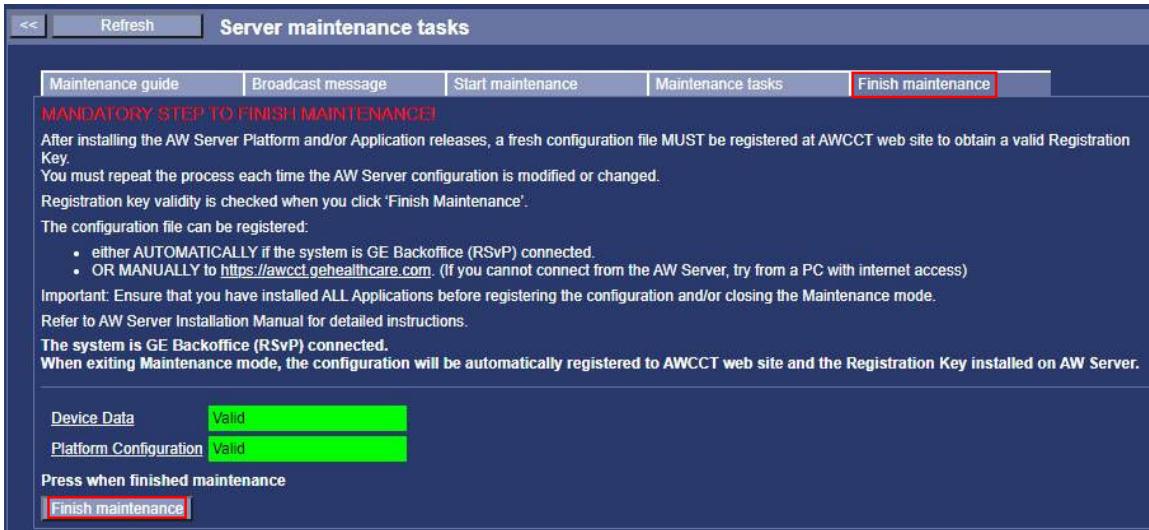
After any maintenance operations on the AW Server (such as upgrading/updating the AW Server, adding/removing Applications, restoring configuration parameters...), exit the Maintenance Mode to unlock the AW Server and allow the AW Server Clients usage.

#### NOTE

In Secured for RMF mode the procedure is the same on the UI, but please note that in the background AW Server will enable SSH and USB for the Maintenance period. When

the user finishes the Maintenance on the Service Tools UI, AW Server in Secured for RMF mode will disable SSH and USB again.

- From the Service Tools, select **Maintenance > Maintenance > Finish maintenance**.



- Carefully read the mandatory conditions to be able to exit from the Maintenance Mode.  
At this stage of the procedure all the mandatory conditions should be met.  
If it is not the case refer to [A.4.2 Exiting the Maintenance mode on page 573](#).
- Click on **Finish Maintenance** button.
- A popup displays, click on **OK** to exit the Maintenance Mode.

# Appendix A Appendices

## A.1 Overview

This chapter contains the following appendices:

- [A.2 Specific field - Characters rules and limitations on page 555](#)
- [A.3 Licensing on page 556](#)
- [A.4 Maintenance Mode on page 571](#)
- [A.5 ClamAV® on page 575](#)
- [A.6 Software Loading Through iLO on page 579](#)
- [A.7 SNMP setup in the iLO service processor on page 588](#)
- [A.8 Useful Commands and Tools on page 589](#)
- [A.9 Filesystem Check on page 595](#)
- [A.10 Hardware Return Procedure on page 599](#)
- [A.11 Physical Servers - Installed Base on page 602](#)

## A.2 Specific field - Characters rules and limitations

This section describes the characters rules and limitations that shall be followed to fill in the **Hostname**, **AE Title**, **IP Address**, **Port**, **System ID**, **Label/Name** and **Smoothing factor** fields.

### 1. AW Server Hostname

- a. The AW Server hostname is restricted to 16 characters maximum.
- b. Only the following characters are supported:
  - [a-z]
  - [0-9]
  - Dash (-)
- c. The hostname shall NOT contain numbers only or start with a number (I.e: hostname = 123456).
- d. The hostname shall NOT contain space(s)
- e. The hostname shall NOT contain dot(s)

#### NOTE

The first dot is considered and used for adding the domain name (if applicable for the site).

<hostname>.<domain\_name> I.e: aws-06.euro.health.ge.com

### 2. AW Server AE Title

- a. The AW Server AE Title is the AW Server Hostname. And as such, as the same characters limitation as for the AW Server Hostname.

### 3. IP Address

- a. 4 numbers/parts (octets)

- b. Numbers [0-255]
- c. Numbers separated by one dot each (i.e : 192.9.100.25)

#### 4. Port

- a. Only numbers [0-9] between 0 and 65535
- b. AW Server use Port # 4006

#### 5. System ID

- a. Only the following is supported:
  - [A-Z]
  - [0-9]
  - underscore (\_)

**NOTE**

System ID cannot contain only zeroes (e.g. 0, 00, 000000, etc...).

#### 6. Label/Name

- a. Only the following characters are supported:
  - [a-z]
  - [A-Z]
  - [0-9]
  - \_ - .

#### 7. Smoothing factor

- a. Only the following characters are supported:
  - [A-Z]
  - [0-9]
  - Underscore (\_) and space

## A.3 Licensing

This section describes:

- The Order Fulfillment and License Generation using eLicense.
- The web-based AW Server Client (Web Client) and the next generation applications License Generation using FlexNet Operations (FNO).

### A.3.1 eLicense licensing

Currently, the AW Server 3.2 Hardware or Virtual server configuration is delivered with:

- 1 Cola License key for the internal License server
- 1 Platform key (8K, 16K, 40K, 80K or 160K slices)
- 1 Pre-processing key (optional)

The following option can be delivered for AW Server 3.2 Hardware or Virtual server configuration:

- 1 Cola License server software package for Windows 7 to load the license server on an external PC (hardware or virtual) + 1 Cola License key for use with external License server.

OR

- 1 Cola License key upgrade for use with an existing Windows XP external License server

The Advanced Applications software packages are delivered with all configurations orders, and license keys will be made available in eLicense depending on the Applications purchased by the site.

### A.3.1.1 eLicense operation

The following is an EXAMPLE of an AW Server initial installation license generation flow from an EXAMPLE stock order. The exact process and flow may vary depending on existing licenses, eLicense website availability / changes, and order details.

Also refer to **5537368-1EN** - Floating License 3.3.x Installation Manual, for more details.

1. Access the eLicense site

<http://elicense.gehealthcare.com/elicense/> OR <http://elicense.gehealthcare.com/>

this second URL is available via the Internet, and via the GEHC VPN connectivity model.

#### NOTE

NOTE THAT THE PROPER ORDER NUMBER WILL BE REQUIRED:

- Global Order Number (GON): \_\_\_\_\_
- No GON available:
  - For end-customers, please contact your GE Service Personnel.
  - GE Service Personnel , please contact your local Support Center or IT ROC

The FE must create an instance corresponding to the model type and then enter the licenseld to be able to generate licenses.

#### Use the following Model Type for AW Server 3.2:

- **AWS\_Primary:** To be used for AW Server 3.2 release
  - Stand Alone AWS Hardware (Hi-tier, or Low-tier) Including Upgrades of existing systems.
  - VM - AWS Stand Alone (No nodes)
  - VM - AWS Primary (first node)
- **AWS\_Node :**Virtual only - All other AWS Nodes on a system.

#### NOTICE

**AWS\_Primary** is the only model-type that will produce a CoLA Server License and individual floating application licenses. It will also produce seat licenses, AutoLaunch, and Integration Licenses. **AWS\_Node** only generates, seat licenses, AutoLaunch, and Integration Licenses.

#### DO NOT Use the following Model Type for AW Server 3.2:

- **AWS** - reserved for AWS2.0 and earlier
- 2. In the HOME page (not shown here), enter the order number (GON) under the “Order Management” section in the “Order Number” field – then click on the “Go” button.
- 3. For the “initial” AW Server installation - the “Order Information” screen should display similar as shown below - if there are no licenses created from this order yet.
  - If there are license(s) created from this order, there will be “KEY” icons in the table – indicating the license key existence.
  - In the below example, the AW Server node-lock slice license is the upgrade catalog license, which is in reality the 40,000 slice license.

- The single AW Server Catalog entry will create TWO NODE-LOCK licenses: The 8K or 16K or 40K or 80K or 160K Platform Enabler & the CoLA License Server Enabler.

## Order Information

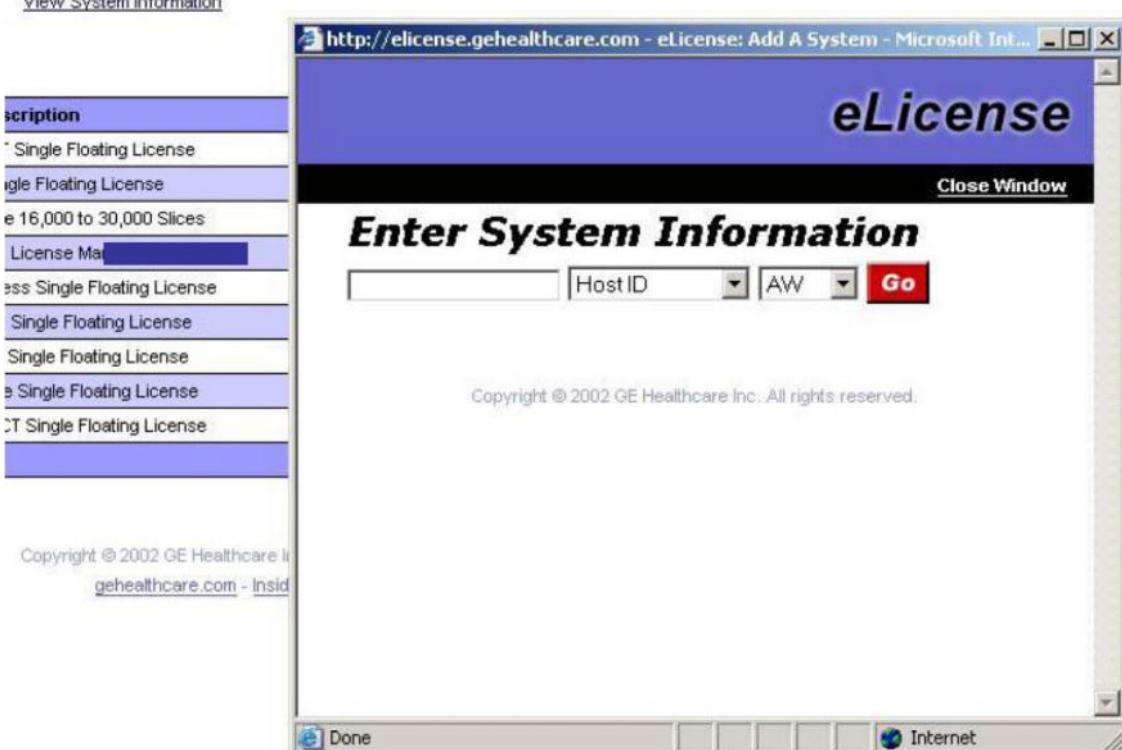
Site: GEHC NPI  
Order Number: 2625216074

**Instructions**  
[Add A System](#)  
[Generate Licenses](#)  
[View System Information](#)

| <b>Add a System</b> |                                                |           |             |          |  |
|---------------------|------------------------------------------------|-----------|-------------|----------|--|
| Catalog Number      | Description                                    | Floatable | Qty Ordered | Qty Used |  |
| P51801BT            | CardIQ Fusion PET Single Floating License      | Y         | 5           | 0        |  |
| P50821CD            | PET VCAR Single Floating License               | Y         | 5           | 0        |  |
| B79821TC            | CardIQ Function Xpress Single Floating License | Y         | 5           | 0        |  |
| M81521AH            | Autobone Xpress Single Floating License        | Y         | 5           | 0        |  |
| B77121VE            | VesselIQ Xpress Single Floating License        | Y         | 5           | 0        |  |
| B79821SH            | CardIQ Xpress Elite Single Floating License    | Y         | 5           | 0        |  |
| M81531ST            | AW Server Upgrade 16,000 to 30,000 Slices      | N         | 1           | 0        |  |
| H25801BT            | CardIQ Fusion SPECT Single Floating License    | Y         | 5           | 0        |  |

- Click on the “Add a System” button. The following screen should display.

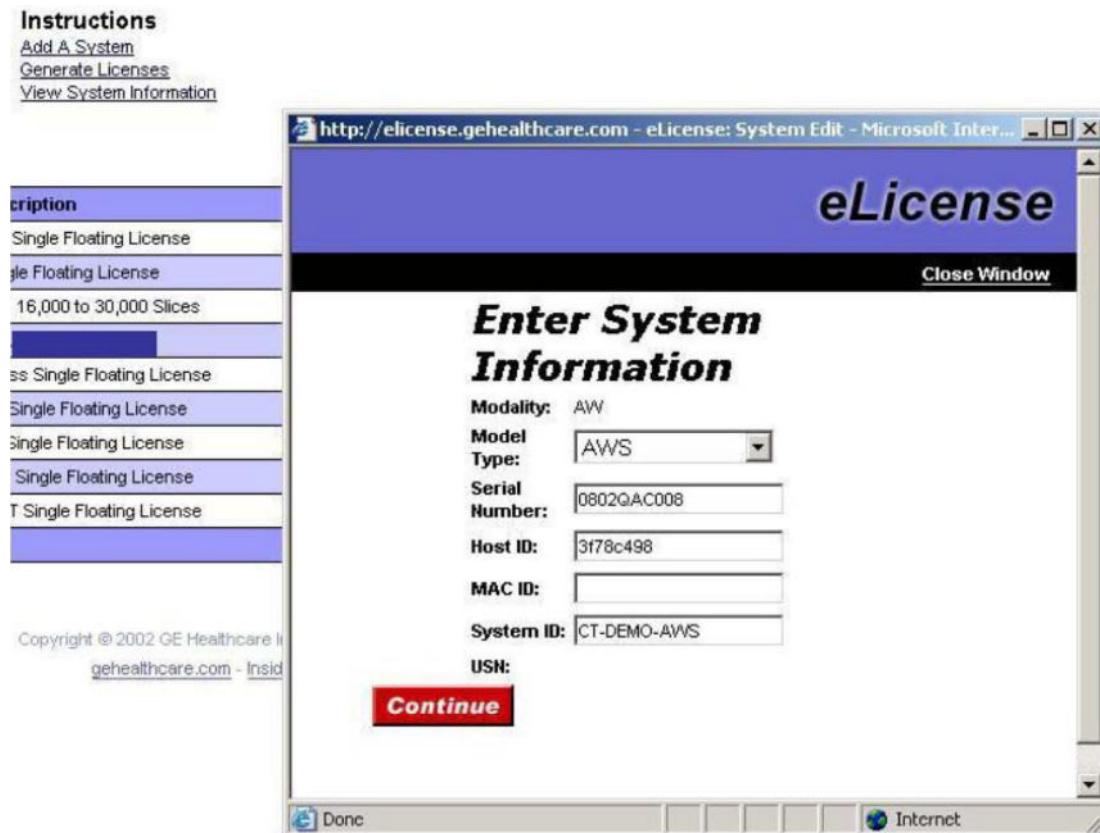
**Instructions**  
[Add A System](#)  
[Generate Licenses](#)  
[View System Information](#)



The screenshot shows a list of license descriptions on the left, with 'Single Floating License' selected for the AW Server. The main window title is 'eLicense' and it displays 'Enter System Information'. It has fields for 'Host ID' (set to 'AW') and a 'Go' button. The bottom of the window includes copyright information and a 'Done' button.

| Description                 |
|-----------------------------|
| Single Floating License     |
| Single Floating License     |
| e 16,000 to 30,000 Slices   |
| License Ma                  |
| ess Single Floating License |
| Single Floating License     |
| Single Floating License     |
| e Single Floating License   |
| CT Single Floating License  |

- Here is where you need to enter the licenseID of the AW Server that you intend to license – this is the Ethernet MAC generated value which is automatically calculated in the Service Tools > Initial configuration > **Licensing tool** under **Platform Configuration > License ID**.
- After entering the licenseID in the above “Enter System Information” field, and making sure that the “HostID” and “AW” pull-downs are selected – the following screen should display.



5. Enter ALL the information requested here.

- The Serial Number of the server should be available on the chassis or in the documentation provided by the vendor.
- The MAC ID was accessed back in the installation section of this document - using the command-line **ip** utility.
- The SYSTEM ID is assigned by the local service team.

**NOTE**

ALL of this information is essential. Please make sure to enter it!

6. Click on the **Continue** button, and the following screen should display.

## ***Order Assignment***

**Site:** GEHC NPI  
**Order Number:** 2625216074

## **Instructions**

[Add A System](#)  
[Generate Licenses](#)  
[View System Information](#)

[Add a System](#) [Generate Licenses](#)

| Host : 3f78c498 <a href="#">Details</a><br>System : 521AWECTDEMO<br>Serial Number : 08020AC008<br>Modality : AW<br>Model Type : AWS<br>(License Server) | Catalog Number | Description                                    | Floatable | Qty Ordered | Qty Used |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------|-----------|-------------|----------|
| <input type="checkbox"/> Check All                                                                                                                      |                |                                                |           |             |          |
| <input type="checkbox"/>                                                                                                                                | P51801BT       | CardIQ Fusion PET Single Floating License      | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | P50821CD       | PET VCAR Single Floating License               | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | B79821TC       | CardIQ Function Xpress Single Floating License | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | M81521AH       | Autobone Xpress Single Floating License        | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | B77121VE       | VesselIQ Xpress Single Floating License        | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | B79821SH       | CardIQ Xpress Elite Single Floating License    | Y         | 5           | 0        |
| <input type="checkbox"/>                                                                                                                                | M81531ST       | AW Server Upgrade 16,000 to 30,000 Slices      | N         | 1           | 0        |
| <input type="checkbox"/>                                                                                                                                | H25801BT       | CardIQ Fusion SPECT Single Floating License    | Y         | 5           | 0        |
| <input type="checkbox"/> Check All                                                                                                                      |                |                                                |           |             |          |

- In this “**Order Assignment**” screen, select the licenses that you want to create for the system that you just previously ADDED, and is now shown in the left part of the table. Check the boxes, or select **Check All** if all the catalog entries on this screen are for the AW Server system entered.

7. Click on the **Generate License** button. The following screen should display.

**Click on the **Generate List** button.**

**Site:** GEHC NPI

| Product                                                                                                                                     |             | Assigned Catalog Items                         |           |                                  |                    |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------------|-----------|----------------------------------|--------------------|
|                                                                                                                                             | Catalog No. | Description                                    | Floatable | Quantity                         | Quantity Available |
| <b>Host : 3f78c498<br/>System : 521AWECTDEMO<br/>Serial Number : 0802QAC008<br/>Modality : AW<br/>Model Type : AWS<br/>(License Server)</b> | P51801BT    | CardIQ Fusion PET Single Floating License      | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | P50821CD    | PET VCAR Single Floating License               | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | B79821TC    | CardIQ Function Xpress Single Floating License | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | M81521AH    | Autobone Xpress Single Floating License        | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | B77121VE    | VesselIQ Xpress Single Floating License        | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | B79821SH    | CardIQ Xpress Elite Single Floating License    | Y         | <input type="button" value="5"/> | 5                  |
|                                                                                                                                             | M81531ST    | AW Server Upgrade 16,000 to 30,000 Slices      | N         | 1                                | 1                  |
|                                                                                                                                             | H25801BT    | CardIQ Fusion SPECT Single Floating License    | Y         | <input type="button" value="0"/> | 5                  |

**Note:**

**Note:** The initial quantity in the "Quantity Selection" box is the maximum number of concurrent users the system supports. You can add more from a different quantity. The quantity you select represent the total number of concurrent users the system will support. For Example, if the box is "3" and you select quantity as "5", that means "2" of them will be from the current order.

- The **Select Quantity** - you will select the number of Floating License instances you will license applications for. The only licenses that will show a quantity select pull-down are floating licenses. Node-locked licenses will (by definition) only show a qty of 1 - no pull-down to change that.

8. Use the “Quantity” column pull-downs to select the number the order has defined for this particular system. In the example, the initial Order Information screen showed a quantity

of 5 each, so select the 5 in the pull-down menu, then click on the "Continue" button. The following screen should display.

## Order Information

Site: GEHC NPI  
Order Number: 2625216074

| PRODUCT                              | ASSIGNED CATALOG ITEMS |                                                |           |          |
|--------------------------------------|------------------------|------------------------------------------------|-----------|----------|
|                                      | Catalog No.            | Description                                    | Floatable | Quantity |
| Host : 3f78c498                      | P51801BT               | CardIQ Fusion PET Single Floating License      | Y         | 5        |
| System : 521AWECTDEMO                | P50821CD               | PET VCAR Single Floating License               | Y         | 5        |
| Serial Number : 0802QAC008           | B79821TC               | CardIQ Function Xpress Single Floating License | Y         | 5        |
| Modality : AW                        | M81521AH               | Autobone Xpress Single Floating License        | Y         | 5        |
| Model Type : AWS<br>(License Server) | B77121VE               | VesselIQ Xpress Single Floating License        | Y         | 5        |
|                                      | B79821SH               | CardIQ Xpress Elite Single Floating License    | Y         | 5        |
|                                      | M81531ST               | AW Server Upgrade 16,000 to 30,000 Slices      | N         | 1        |
|                                      | H25801BT               | CardIQ Fusion SPECT Single Floating License    | Y         | 5        |

**Confirm Selection(s)**

**Back**

- The "Order Information" screen now shows all the catalog licenses that have been created for the system, and their quantities. Notice the "Floatable" column – the server 'node lock' slices license is NOT floatable – it is NODE-LOCKED to this node/system.
- If the data in this table is all correct, click the "**Confirm Selection(s)**" button, and the following screen should display.

## Order Assignment

Site: GEHC NPI  
Order Number: 2625216074

### Instructions

[Add A System](#)  
[Generate Licenses](#)  
[View System Information](#)

**Add a System**    **Generate Licenses**

| Host : 3f78c498 <a href="#">Details</a><br>System : 521AWECTDEMO<br>Serial Number : 0802QAC008<br>Modality : AW<br>Model Type : AWS<br>(License Server) | Catalog Number | Description                                    | Floatable | Qty Ordered | Qty Used |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------|-----------|-------------|----------|
| <input type="checkbox"/> All                                                                                                                            | P51801BT       | CardIQ Fusion PET Single Floating License      | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | P50821CD       | PET VCAR Single Floating License               | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | B79821TC       | CardIQ Function Xpress Single Floating License | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | M81521AH       | Autobone Xpress Single Floating License        | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | B77121VE       | VesselIQ Xpress Single Floating License        | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | B79821SH       | CardIQ Xpress Elite Single Floating License    | Y         | 5           | 5        |
| <input type="checkbox"/> All                                                                                                                            | M81531ST       | AW Server Upgrade 16,000 to 30,000 Slices      | N         | 1           | 1        |
| <input type="checkbox"/> All                                                                                                                            | H25801BT       | CardIQ Fusion SPECT Single Floating License    | Y         | 5           | 5        |

- The "Order Assignment" screen will now show "KEY" icons in the left part of the table. This means that "license keys" have been created for the catalog items listed in the row where the KEY icon displays.
  - To examine the actual licenses, and access the options to save or print them – click on the "Details" button in the top of the left part of the table where the system details are shown. The following example screen should display.

### System Information

Edit System Information  
**Modality:** AW  
**Model Type:** AWS  
**Serial Number:** 0802GAC008  
**Host ID:** 3178c498  
**System ID:** S21AWEECTDEMO  
**USN:** 000135490

**Instructions**  
[Generate New Licenses](#)  
[Email Licenses](#)  
[Save Licenses](#)  
[Print Licenses](#)  
[Update List](#)  
[Reconfigure System](#)

|                          |               | <a href="#">Generate New Licenses</a> |          | <a href="#">Email Licenses</a> |            | <a href="#">Save Licenses</a>                  |           | <a href="#">Print Licenses</a> |                     | <a href="#">Update List</a> |             | <a href="#">Reconfigure</a> |          |
|--------------------------|---------------|---------------------------------------|----------|--------------------------------|------------|------------------------------------------------|-----------|--------------------------------|---------------------|-----------------------------|-------------|-----------------------------|----------|
| Delete                   | Generate Date | Generate Type                         | Order ID | Genesis ID                     | Catalog ID | Description                                    | Floatable | Application Name/Key           | Number of Users     | Generated By                | Modified By | Modified Date               | Download |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | H25801BT   | CardIQ Fusion SPECT Single Floating License    | Y         | CardIQ_Fusion_SPECT            | DT9D9T73E4OUY2G7 5  | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | B79821TC   | CardIQ Function Xpress Single Floating License | Y         | CardIQ_Function_Xpress         | SP836DQYFCUVQ2K8 5  | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | M81531ST   | AW Server Upgrade 16,000 to 30,000 Slices      | N         | SdC_Server_Eight_Slices        | M9C97JZPPPOYC37P 1  | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | B79821SH   | CardIQ Xpress Elite Single Floating License    | Y         | CardIQ_Xpress_Elite            | SYTSSLRPM770CN77 5  | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | M81521AH   | Autobone Xpress Single Floating License        | Y         | AutoBone_Xpress                | FAYZEDLHDDLR8YQH3 5 | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | P50821CD   | PET VCAR Single Floating License               | Y         | PET_VCAR                       | C3DQH78DN4T3B92 5   | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | P51801BT   | CardIQ Fusion PET Single Floating License      | Y         | CardIQ_Fusion_PET              | BHYBV2XPLT9AFSA 5   | 212007031                   | 212007031   | 2009-02-16                  |          |
| <input type="checkbox"/> | 2009-02-16    | Generated From Order                  | N/A      | 2625216074                     | B77121VE   | VesselIQ Xpress Single Floating License        | Y         | VesselIQ_Xpress                | JW776XEP4EU2J98 5   | 212007031                   | 212007031   | 2009-02-16                  |          |

The AW Server "SLICES" catalog creates TWO node-lock licenses:  
The Platform Enabler & the Server Enabler (CoLA License Server)

- An “example” CoLA License key is DT9D9T73E4OUY2G7 5

The number "5" is not part of the license. It is the number of users licenses available.

10. The “System Information” screen now shows the list of licenses that have been created for the specified system.

- The above example screen is only a low-resolution example to show the general structure of the information. Your eLicense session will be much easier to read.
- Notice the buttons at the top of the table.
  - Generate New Licenses** – This is to “manually” generate new licenses without an order number. This is only available for eLicense ADMIN users. Do not use this in the FIELD.
  - Email Licenses** – This will allow you to e-mail the license file.
  - Save Licenses** – This will allow you to download and save the license file to your local file-system.
  - Print Licenses** – This will allow you to print a hard copy of the licenses file.
  - Update List** – This tool is available to manually update the applications list in eLicense with licenses that may exist on the system, but do not exist on the eLicense page for whatever reason. There should be no reason to use this option for this product – DO NOT USE.
  - Reconfigure** - This is only available for eLicense ADMIN users. Do not use this in the FIELD if it appears.

**NOTE**

The above list of eLicense options is an “Administrative” Role list. Some of these options will not even appear on the eLicense interface for “standard” field users.

### A.3.1.2 Converting Node-Locked to Floating

For the following feature, careful communication between Sales, Service and the Customer is needed to identify what options are to be converted before starting. Also that all options on the old system exist in the eLicense database.

There is now a commercial offering that will allow licenses that are currently calculated as node-locked on an AW model system to be converted and moved to a Licenses Server as Floating Licenses. When the relevant Catalog is selected, eLicense displays a pop-up similar to the **Hardware Upgrade** screen described above. The difference is that the **TO: system** will always be a Floating License Server (AWS\_Primary, or License Server) model-type.

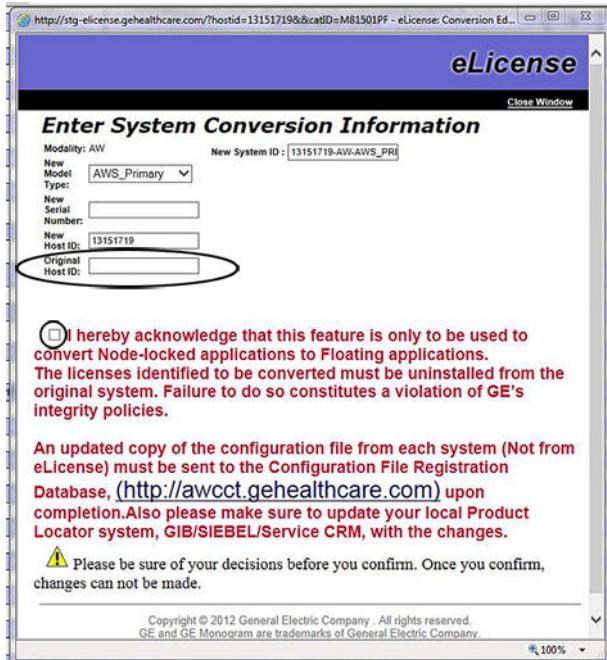
It is also possible to move individual line item options, rather than the entire set of licenses for the system (as is the case in the Hardware Upgrade). In other words, some software options may be left with Node-locked license keys on a specific AW system that will be staying on site.

As was the case for a Hardware upgrade, ensure that all of the licenses that exist on the workstation today are listed in eLicense before starting this process.

The procedure is very similar to the Hardware upgrade procedure. Select the single catalog for converting options from node-locked to:

| Order Assignment                                                 |                |                                       |                              |                                   |                                         |
|------------------------------------------------------------------|----------------|---------------------------------------|------------------------------|-----------------------------------|-----------------------------------------|
|                                                                  |                |                                       | Instructions                 |                                   |                                         |
|                                                                  |                |                                       | <a href="#">Add A System</a> | <a href="#">Generate Licenses</a> | <a href="#">View System Information</a> |
| Host : 3a879e65                                                  | Catalog Number | Description                           | Floatable                    | Qty Ordered                       | Qty Used                                |
| Header ID : 14925979                                             |                |                                       |                              |                                   |                                         |
| Site: VALLEY VIEW MEDICAL CENTER                                 |                |                                       |                              |                                   |                                         |
| Address: VALLEY VIEW MEDICAL CENTER                              |                |                                       |                              |                                   |                                         |
| Street:                                                          |                |                                       |                              |                                   |                                         |
| City, State, Zip: FORT MOHAVE,AZ,86426-9225                      |                |                                       |                              |                                   |                                         |
| Country: US                                                      |                |                                       |                              |                                   |                                         |
| <a href="#">Add a System</a>   <a href="#">Generate Licenses</a> |                |                                       |                              |                                   |                                         |
| <input type="checkbox"/> Host : 3a879e65                         |                |                                       |                              |                                   |                                         |
| System :                                                         |                |                                       |                              |                                   |                                         |
| Serial Number : 2ua1130dsk                                       |                |                                       |                              |                                   |                                         |
| Modality : AW                                                    |                |                                       |                              |                                   |                                         |
| Model Type : AW46                                                |                |                                       |                              |                                   |                                         |
| <input type="checkbox"/> Check AW                                |                |                                       |                              |                                   |                                         |
|                                                                  | B7500LN        | CONNECTPRO HIS/RIS SW KEY (LINUX)     | N                            | 1                                 | 0                                       |
|                                                                  | B7500PL        | LINUX CONNECTPRO WITH BARCODE READER  | N                            | 1                                 | 0                                       |
|                                                                  | B7540RB        | BAR CODE READER OPTION                | N                            | 1                                 | 0                                       |
| <input type="checkbox"/>                                         | B77021PD       | CT PERF 4D NEURO                      | N                            | 1                                 | 0                                       |
| <input type="checkbox"/>                                         | B79971RT       | REPORTING TOOL SW                     | N                            | 1                                 | 0                                       |
|                                                                  | M80171LE       | CONCURRENCY ENABLER                   | N                            | 1                                 | 0                                       |
| <input type="checkbox"/>                                         | M81521VK       | VOLUME VIEWER 5 MR                    | N                            | 1                                 | 0                                       |
|                                                                  | M81521VL       | VOLUME VIEWER 5 PET                   | N                            | 2                                 | 0                                       |
| <input type="checkbox"/>                                         | M81061CF       | Convert Existing Licenses to Floating | N                            | 1                                 | 0                                       |
| System Conversion Upgrade Complete                               |                |                                       | AW VOLUMESHARE 5-SW UPGRADE  | N                                 | 1                                       |

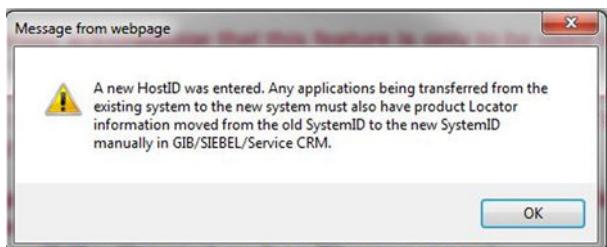
There will be one check box to select the Conversion. When this box is selected, a new window will launch as displayed below. (Catalog will be M81061CF).



At this point enter the **licenseID** of the Original Host ID similar to what was performed on Hardware upgrade. This is the system that you will be transferring licenses from. You will not use original SystemID as this process allows moving only some applications and the existing system remains in operation with the Customer. Then acknowledge that this is being used to convert from Node-locked to Floating.

As with the Hardware Upgrade, a **Continue** button will then display allowing license calculation process to continue.

Once again, a reminder pop-up will display to have the user update the region Product Locator system showing the options removed from the old system and being re-installed on the new system.



New features may also be added to the server at the same time as conversion is taking place. There also may be more than one conversion catalog on the order as the Customer may want to convert options from multiple workstations. If this is the case, the quantity of the Convert catalog should match the number of workstations to have options converted from. The appropriate quantity of new options to be installed on the server, and a quantity of one convert should be selected for each workstation to be used for Conversion.



[Home](#) | [Admin](#) | [User Guide](#) | [Version](#) | [Feedback](#) | [Logout](#)

## Select Quantity

Site: VETERANS AFFAIRS MEDICAL CENTER  
FDO: 31827341 / 4179334  
Order Date: 2015-12-01  
Billing Number: 99142  
Address: VETERANS AFFAIRS MEDICAL  
Street: CENTER  
City, State Zip: DALLAS,TX,75216-7167  
Country: US

| PRODUCT                                                                                                                            | ASSIGNED CATALOG ITEMS |                              |           |                                  |                    |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------|------------------------------|-----------|----------------------------------|--------------------|
|                                                                                                                                    | Catalog No.            | Description                  | Floatable | Quantity                         | Quantity Available |
| Host : 3ba07626<br>System : AWSCAVE<br>Serial Number : USE308WJA3<br>Modality : AW<br>Model Type : AWS_Primary<br>(License Server) | M81501PF               | AWE LOW TIER POWER CORDS KIT | Y         | <input type="button" value="1"/> | 1                  |
|                                                                                                                                    | M81551VR               | Volume Viewer SFL            | Y         | <input type="button" value="8"/> | 3                  |

**Continue** **Back**

**Note:**  
The initial quantity in the "Quantity Selection" box is the maximum number of concurrent users the system supports. You can add more from this order by selecting a different quantity. The quantity you select represent the total number of concurrent users the system will support. For Example, if the initial value in the selection box is "3" and you select quantity as "5", that means "2" of them will be from the current order.

Copyright © 2012 General Electric Company . All rights reserved.  
GE and GE Monogram are trademarks of General Electric Company.  
[gehealthcare](#) a division of General Electric Company

A list of options available on the **From:** system will display with radial buttons to select options for conversion.

[Home](#) | [Admin](#) | [User Guide](#) | [Version](#) | [Feedback](#) | [Logout](#)

## Conversion Selection

Site: WILKES BARRE GENERAL HOSPITAL  
FDO: 2990727  
Order Date: 2012-02-08  
Address: WILKES BARRE GENERAL HOSPITAL  
Street:  
City, State Zip: WILKES BARRE,PA,18702-2634  
Country: US

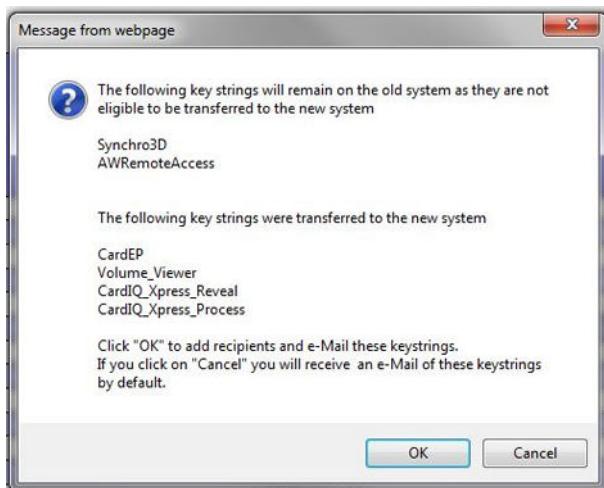
| Original System                                                                                | New System                                                                                                                     | Licenses                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host: 3a254588<br>System: BRIT<br>Serial Number: 2ua90417b<br>Modality: AW<br>Model Type: AW46 | Host: 73d26cd2<br>System: HPML350G6_CSELAB<br>Serial Number: USE946N3D8<br>Modality: AW<br>Model Type: AWS<br>(License Server) | <input type="checkbox"/> ARSdC<br><input checked="" type="checkbox"/> CardIQ_Xpress_Elite<br><input type="checkbox"/> CardIQ_Xpress_Pro<br><input checked="" type="checkbox"/> VesselIQ_Xpress<br><input type="checkbox"/> AdvantageSim<br><input type="checkbox"/> SimMD_AutoSeg |

**Confirm Selection(s)** **Back**

After selecting the items to be converted from the AW (node-Locked system) confirm the selections then you will be directed to a quantity selection page if you have additional new catalog items that were selected on the order to also be added to the system.

The screenshot shows the 'Order Information' section of the eLicense software. It displays details for a host ID (08358180) and a new system (73d26cd2). A table lists assigned catalog items, including CT PERFD UNIROL SFL, VESSELIO XPRESS SINGLE FL, and Convert Existing Licenses to Floating. Below the table, a message box says: 'The following key strings will remain on the old system as they are not eligible to be transferred to the new system: Synchro3D, AWRemoteAccess'. Another section lists transferred key strings: CardEP, Volume\_Viewer, CardIQ\_Xpress\_Reveal, and CardIQ\_Xpress\_Process. A note at the bottom says: 'Click "OK" to add recipients and e-Mail these keystrings. If you click on "Cancel" you will receive an e-Mail of these keystrings by default.' Buttons for 'Confirm Selection(s)' and 'Back' are visible.

A pop-up will display advising the keystrings that will be converted and added into any existing quantity on the AW Server. It will also display a list of any options that were selected for convert, but are not eligible to convert as these keystrings do not function on the Server products. As is the case with Hardware Upgrade, if some of the features selected individually.



In the same manner as for Hardware Upgrade, an email will be sent to the user, and the option to add additional e-mail recipients for this communication will be available.

Once the selections are confirmed, a key icon will display advising that the Conversion is complete. Click on the HostID Hot-link of the New System to confirm the desired licenses have been moved and added appropriately to any existing quantity, and any new options that were selected as well. Also searching on the Original system hostID should confirm that the selected options no longer exist on that system.



During the process, if you select a line item from the Original System that has a keystring that does not function in a floating license mode, an error message will display advising the user of this situation.

## A.3.2 Flexera Licensing

To license the web-based AW Server Client (Web Client) and the next generation applications, a specific licenses file must be installed into the AW Server. These licenses are based on the License ID and the licenses file is generated using FlexNet Operations (FNO).

The AW Server 3.2 entitlement(s) have already been created for your site in FNO (through automatic mechanism), and associated to the customer account. This procedure describes how to create a device and generate the licenses file.

### A.3.2.1 FlexNet Operations (FNO)

The licenses generation is based on the License ID of the AW Server and the generated licenses file name is of the form <License\_ID>.bin.

#### NOTE

If the correct GE person is not associated with the customer account, device creation and entitlement association is not possible. If you encounter this situation in the below steps, enter a ticket in **MyTech** ([mytech.ge.com](http://mytech.ge.com)) by selecting **Help & Support** and **searching for eDelivery as business application**. In the support page, create the ticket with the description mentioning that you want to be linked to the account created to the GON.

1. Log into the FlexNet Operations (FNO) site: <https://gehealthcare.flexnetoperations.com/flexnet/operationsportal/logon.do>
2. To create a new device:

- a. Select **Devices > Create Device**.

The screenshot shows the GE Healthcare License & Delivery Portal. At the top, there's a navigation bar with links for Home, Activation & Entitlements, License Support, Devices (which is highlighted with a red box), Usage, Downloads, and Accounts & Users. Below the navigation bar, there's a sub-navigation menu for 'Devices' with options 'Create Device' (also highlighted with a red box) and 'Offline Device Management'. On the left side, there's a sidebar titled 'Your Downloads' with a single item 'AW'. The main content area is titled 'Recent Entitlements' and lists three entries:

| Activation ID          | Product                                    | Last modified |
|------------------------|--------------------------------------------|---------------|
| 7ae6-b798-e0d0-4fa8... | cvi42 5.11 ext. 2 for service              | Nov 1, 2022   |
| ec16-2c81-a0f0-45ec... | AW Server 3.2 Ext. 4.0 for Service         | Nov 1, 2022   |
| 0175-1780-7adc-40dd... | Volume Viewer Apps 15.0 Ext. 8 for Service | Nov 1, 2022   |

- b. Fill in the device details according to the following:

The screenshot shows the 'Device New Device' configuration form. It includes fields for Name (set to 'BUCAW239'), Runs license server? (unchecked), Model (set to 'FLX\_CLIENT\_GEHC (default)'), ID Type (set to 'STRING'), ID (set to '068a1f01'), Account (set to 'AW SERVICE ENGINEERING (A)'), Site name (set to 'Buc'), and a 'Save' button at the bottom.

**Name:** Device name. Use the System ID (CRM Number).

**Run license server?**: Leave unchecked.

**Model:** *FLX\_CLIENT\_GEHC (default)*

**ID Type:** STRING

**ID:** License ID of the AW Server.

**Account:** Customer account.

**Site name:** Not required.

- c. Click on **Save** button.

3. To use an existing device:

- a. Select **Devices > Device**.

| Activation ID          | Product                                                 | Last modified |
|------------------------|---------------------------------------------------------|---------------|
| fcd7-66ba-10b0-4bbf... | 5779605SSW Quantib Brain 1.4 for service                | Nov 8, 2022   |
| 2deb-30c0-8afc-47aa... | 5780008SSW CardIQ Xpress Process 2.3 Ext. 6 for service | Nov 8, 2022   |
| 7ae6-b798-e0d0-4fa8... | 5779601-7SSW cvi42 5.11 ext. 2 for service              | Nov 1, 2022   |

- b. Search for the existing device using the search fields.

| Name        | ID                  | Type              | Account                                                             | Licenses     | Updates    | Last Modified |
|-------------|---------------------|-------------------|---------------------------------------------------------------------|--------------|------------|---------------|
| Fred Jensen | 262577VCT1 (STRING) | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT (GEHC AW SERVICE INTERNAL ACCOUNT) | No licenses  | No updates | Oct 31, 2022  |
| bucaw70-239 | 068a1f01 (STRING)   | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT (GEHC AW SERVICE INTERNAL ACCOUNT) | License Info | No updates | Oct 31, 2022  |
| Mangala AW  | 4310bd77 (STRING)   | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT (GEHC AW SERVICE INTERNAL ACCOUNT) | No licenses  | No updates | Oct 30, 2022  |
| Los Cobos   | mr4479coaw (STRING) | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT (GEHC AW SERVICE INTERNAL ACCOUNT) | No licenses  | No updates | Oct 26, 2022  |
| EBD         | 512SEBDCT (STRING)  | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT (GEHC AW SERVICE INTERNAL ACCOUNT) | No licenses  | No updates | Oct 25, 2022  |
| OLCHPHT     | fb4c8b18 (STRING)   | Standalone Device | GEHC AW SERVICE INTERNAL ACCOUNT                                    | License Info | No updates | Oct 21, 2022  |

- c. Select the device.

4. The **Device** panel displays.

**Device BUCAW70239**

Back to list

Overview    Updates    Downloads

**Action**

**Device Details**

ID : 068a1f01  
 Name: BUCAW70239  
 Site Name: Buc  
 Status: ACTIVE  
 Series: FLX\_CLIENT\_SERIES  
 Model: FLX\_CLIENT\_GEHC  
 Account: AW SERVICE ENGINEERING (AW SERVICE ENGINEERING)  
 Vendor Dictionary : (None)

**Model Details**  
 The device model does not include any pre-installed licenses.  
 No licenses are currently mapped.

**NOTE**

For an existing device, the licenses are mapped in the blue area under **Licenses** headline.

5. Map the licenses:

If no license are mapped or more licenses should be mapped, follow the below steps.

a. Select **Action > Map Entitlements**.

**Device BUCAW70239**

Back to list

Overview    Updates    Downloads

**Action**

**Device Details**

- Map Entitlements
- Map By Activation ID
- Remove Licenses
- Return Device
- Download Capability Response

- b. In the **Map Entitlement** panel, for each entitlement (each row) of the device, put the purchased quantity into the **Qty to Add** field and click on **Save** button.

### Map Entitlements

| ID                              | 068a1f01      |           |         |                                            |                                         |            |
|---------------------------------|---------------|-----------|---------|--------------------------------------------|-----------------------------------------|------------|
| ID Type                         | STRING        |           |         |                                            |                                         |            |
| Name                            | BUCAW70239    |           |         |                                            |                                         |            |
| Account: AW SERVICE ENGINEERING |               |           |         |                                            |                                         |            |
| Qty to add                      | Available qty | Total qty | Maximum | Product                                    | Activation ID                           | Expiration |
| 1                               | 2             | 2         | 2       | B79821DA-EDL , Version 2                   | 8114-b8c1-7d9f-4fe7-88d0-40eb-d33a-c392 | PERMANENT  |
| 1                               | 2             | 2         | 2       | M81601ECED , Version 1                     | 215f-794f-e927-4501-b551-24ab-7302-9ec0 | PERMANENT  |
|                                 | 1             | 1         | 1       | 5928524SSW , Version 1                     | c5e9-e0f7-1ed6-415d-9aea-5351-8923-879a | PERMANENT  |
|                                 | 1             | 1         | 1       | AW eDelivery Install Manager , Version 2.2 | 76c9-e5cd-1878-4727-a20a-42bf-edde-5585 | PERMANENT  |
|                                 | 1             | 1         | 1       | 5873501SSW , Version 4                     | e14e-a117-501d-40a8-9a68-3b47-ce92-e821 | PERMANENT  |
|                                 | 1             | 1         | 1       | 5920646SSW , Version 2                     | 9bce-66ce-d1ce-42d4-980f-ab47-f471-d8dd | PERMANENT  |
|                                 | 1             | 1         | 1       | B79821DAED , Version 2                     | 868f-106e-7daf-4bba-ab66-0dc7-17f5-fb31 | PERMANENT  |
|                                 | 1             | 1         | 1       | 5765005SSW , Version 4                     | f4c9-45b5-cb92-487b-83a8-8bd3-02f1-f7bf | PERMANENT  |
|                                 | 1             | 1         | 1       | 5765005SSW , Version 4                     | 2fc8-a087-b127-4a0e-93f9-181a-c1c8-33ef | PERMANENT  |

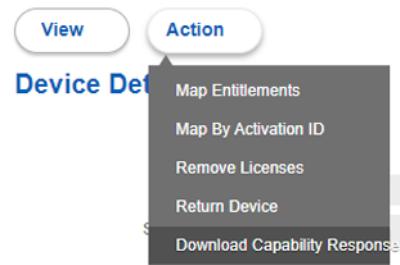
**Save**

6. Generate the licenses file:

- a. Assigned product will appear in the **Device** panel at the **Licenses** area.

| Licenses                 |                                         |                       |            |            |                        |
|--------------------------|-----------------------------------------|-----------------------|------------|------------|------------------------|
| Product                  | Activation ID                           | Status                | Qty mapped | Expiration | Owner                  |
| M81601ECED , Version 1   | 215f-794f-e927-4501-b551-24ab-7302-9ec0 | License not generated | 1          | Permanent  | AW SERVICE ENGINEERING |
| B79821DA-EDL , Version 2 | 8114-b8c1-7d9f-4fe7-88d0-40eb-d33a-c392 | License not generated | 1          | Permanent  | AW SERVICE ENGINEERING |

- b. Download the license file by Selecting **Action > Download Capability Response**.



The licenses file is generated and downloaded to the PC with the name:

<License ID>.bin (for instance: 068a1f01.bin)

- c. Refresh/reload the page. The status of the licenses change to **License generated**.

| Licenses                 |                                         |                   |            |            |                        |
|--------------------------|-----------------------------------------|-------------------|------------|------------|------------------------|
| Product                  | Activation ID                           | Status            | Qty mapped | Expiration | Owner                  |
| M81601ECED , Version 1   | 215f-794f-e927-4501-b551-24ab-7302-9ec0 | License generated | 1          | Permanent  | AW SERVICE ENGINEERING |
| B79821DA-EDL , Version 2 | 8114-b8c1-7d9f-4fe7-88d0-40eb-d33a-c392 | License generated | 1          | Permanent  | AW SERVICE ENGINEERING |

7. Upload the licenses file into the AW Server through the Service tools.

**NOTICE**

The licenses file can be downloaded from FNO and uploaded to the AW Server only for 7 days from its generation.

The same licenses file can be uploaded only once to an AW Server (in case of reinstallation of Licensing/platform, the licenses file can be downloaded several times within the 7 days expiration).

## A.4 Maintenance Mode

The following information describe the steps to enter and exit the Maintenance Mode. The maintenance mode allows the AW Server to be "isolated" from the Clients in order to perform maintenance operations such as adding/removing Applications, or restoring configuration parameters.

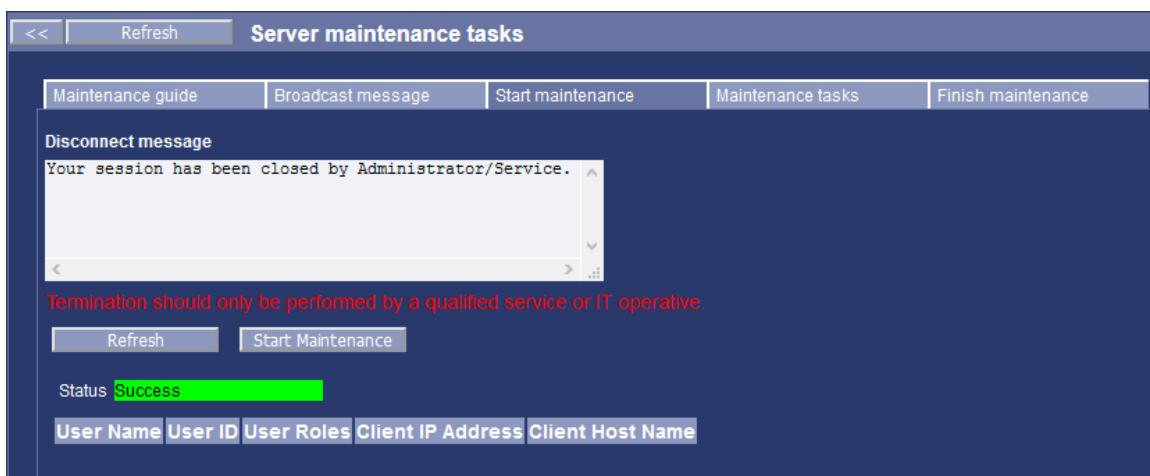
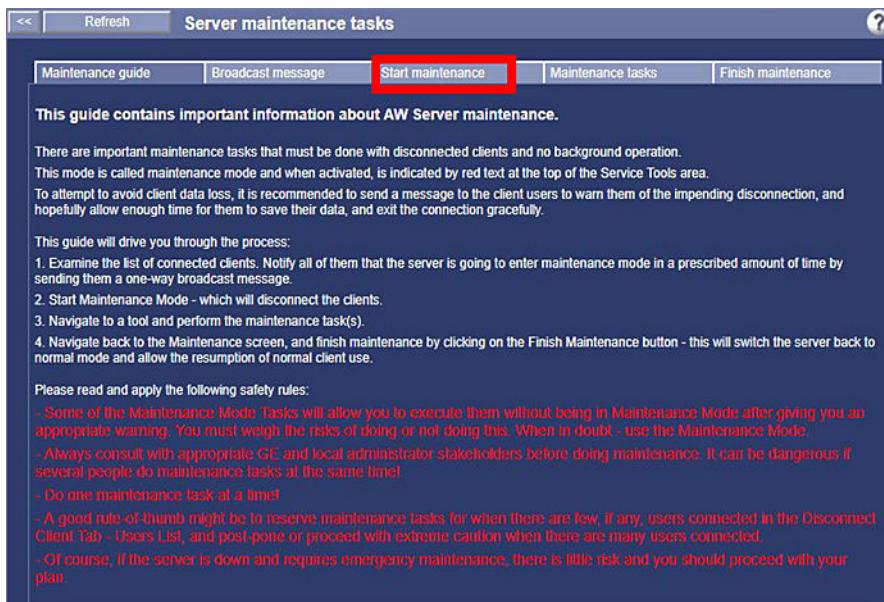
- The AW Server automatically enters the Maintenance mode after software load (Load From Cold). This is also the case for Manufacturing preloaded systems.
- The Maintenance mode is not reset by a reboot.
- The system automatically enters the Maintenance mode at reboot if the Registration status becomes invalid (I.e: expired temporary key)

### A.4.1 Entering the Maintenance mode

**NOTE**

In Secured for RMF mode the procedure is the same on the UI, but please note that in the background AW Server will enable SSH and USB for the Maintenance period. When the user finishes the Maintenance on the Service Tools UI, AW Server in Secured for RMF mode will disable SSH and USB again.

1. Connect to the server and launch the Service Tools (login as **service**).  
The **Version Management** tool which allows installing or upgrading Applications must be used in Maintenance mode.
2. From the Service Tools menu, click on **Maintenance > Maintenance**.  
The *Server maintenance tasks* panel displays.
3. Click on the **Start Maintenance** tab.



#### 4. Check if users are connected.

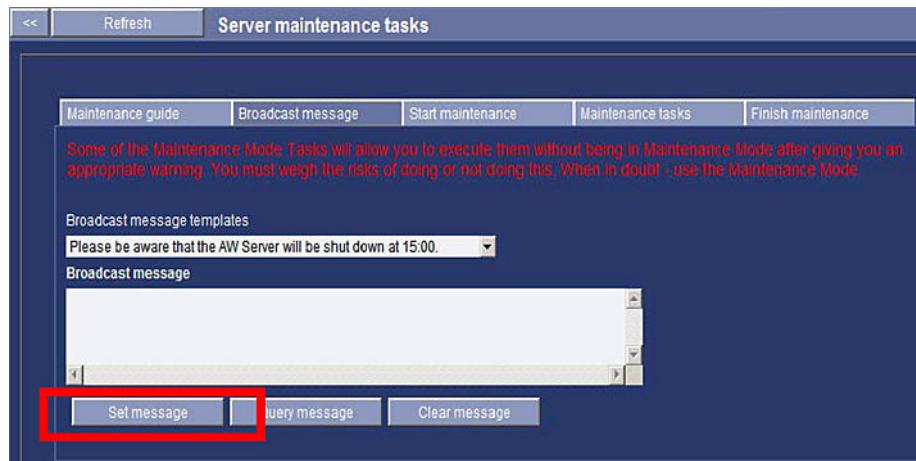
The example below shows two users connected.

| Status Success |         |            |                   |                                      |
|----------------|---------|------------|-------------------|--------------------------------------|
| User Name      | User ID | User Roles | Client IP Address | Client Host Name                     |
|                | voxaf   | [STANDARD] | 3.213.160.218     | awpc218                              |
|                | voxaf   | [STANDARD] | 192.168.0.37      | HCE-4K5PR4J.clients.em.health.ge.com |

#### 5. If any user is connected, send a broadcast message:

- Click on the **Broadcast message** tab.
- Write a message or modify the default message to adapt it to your needs.

- c. Click on **Set message** to broadcast it.

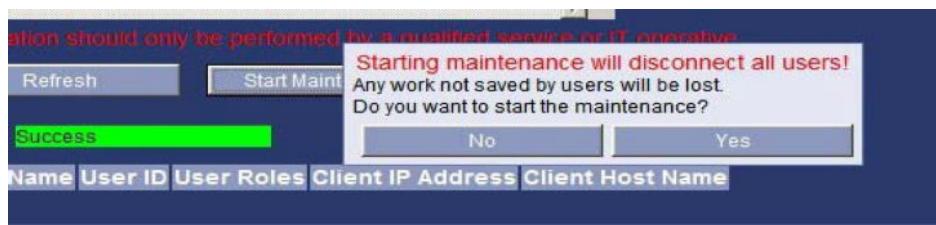


#### NOTICE

Allow a grace delay (a few minutes) for the users to save their work before disconnecting them by entering the Maintenance mode.

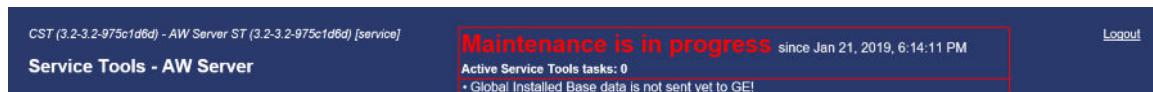
6. Click on the **Start maintenance** tab and on **Start maintenance**.

A pop-up confirmation message appears.



7. Click on **Yes**.

Another pop-up states that you are in maintenance mode.

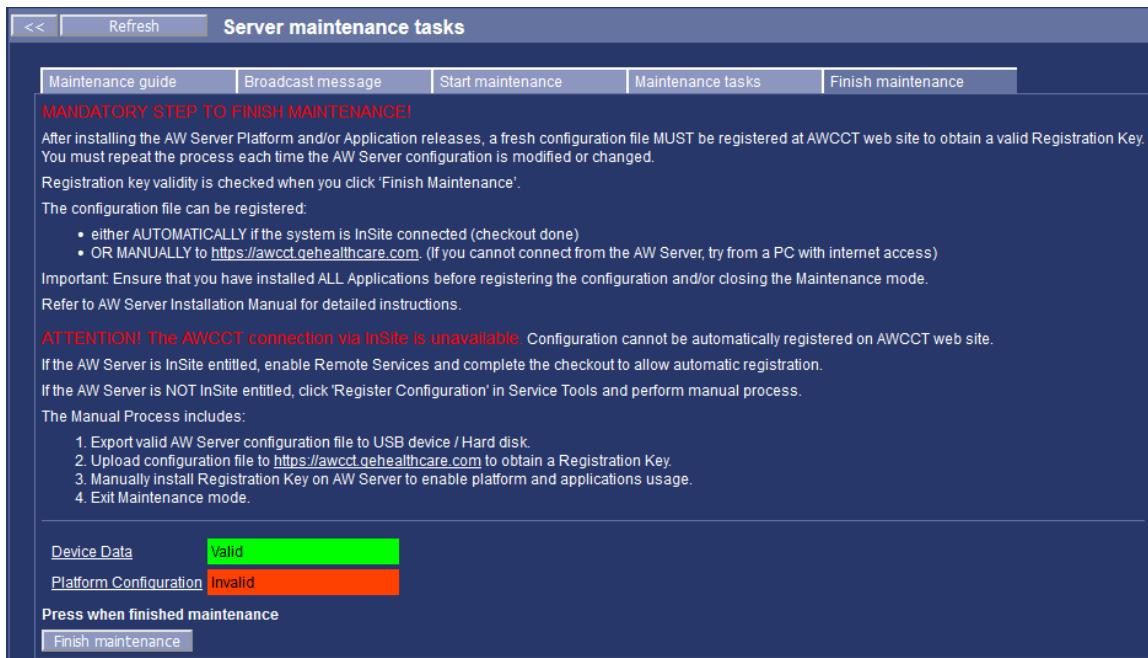


## A.4.2 Exiting the Maintenance mode

#### NOTE

In Secured for RMF mode the procedure is the same on the UI, but please note that in the background AW Server will enable SSH and USB for the Maintenance period. When the user finishes the Maintenance on the Service Tools UI, AW Server in Secured for RMF mode will disable SSH and USB again.

- In the Service maintenance tasks panel, click on the **Finish maintenance** tab.



- Carefully read the mandatory conditions to be able to exit from the Maintenance mode.

### 3. NOTE

The Device data and Platform Configuration setup must be complete before exiting Maintenance.

Check if the Device Data and Platform Configuration setup are complete.

If it is complete, **Valid** is displayed with a green background. If it is not complete, **Invalid** is displayed with a red background.

- If the Device Data and/or Platform Configuration setup are not complete, click on **Device Data** and/or **Platform Configuration** to complete them.

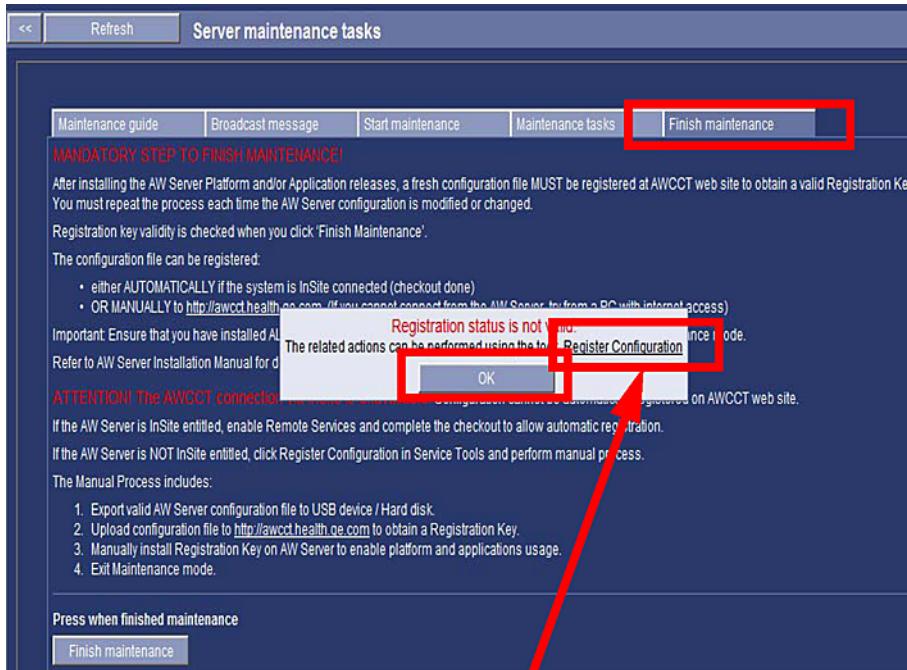
See [2.15.3 Device Data on page 146](#) and [2.15.9 Platform Configuration on page 153](#) for details.

- If there are still some background processes running (I.e: database recovery), the number and name of active processes (maintenance tasks) are displayed on top of the Service Tools. In that case, you will have to acknowledge the message asking you to confirm that you want to force exiting the Maintenance mode.

### 6. NOTE

The AW Server must be properly registered and get its registration key before exiting the Maintenance mode.

If the configuration has not been properly registered, the error message **Registration status is not valid.** displays.



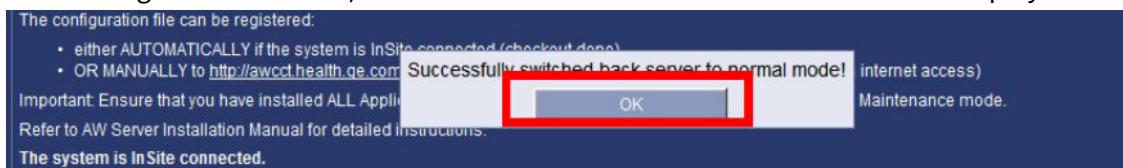
- To enter the *Register Configuration* menu, click on the link as shown above, or on the **Register Configuration** menu link.

Refer to [2.22 Job Card IST013 - System Configuration Registration on page 259](#) for detailed steps of Register Configuration tool.

- To exit and return to the *Maintenance mode* main menu, click on **OK**.

## 7. Click on the **Finish Maintenance** button.

The message **Successfully switched back server to normal mode!** displays.



## 8. Click on **OK** to acknowledge.

### NOTE

There may be cases where the Maintenance mode mentions (and lists) that there are still some tasks running, and that terminating the Maintenance mode may stop them. However, you can decide to force the end maintenance process.

## A.5 ClamAV®

### NOTE

This Appendix does not apply to AW Server Secured for RMF mode

An antivirus package called ClamAV® (Clam AntiVirus®) is bundled with the AW Server operating system.

**By default the antivirus is not activated** but in some circumstances, customers may request that it is activated. However, the need for antivirus on Linux-based systems such as the AW Server is debatable for the following reasons:

- Linux built-in permissions apply to every file on the system, and cover read, write and execute. Typically, software that can impact the system as a whole requires root privileges to run.

- Linux does not rely on file extensions to determine file properties; this avoids accidental launch of malware.
- Unlike Windows™, Linux does not allow outsiders to execute software on the system (although RSvP is an exception to this).
- The AW Server is installed with a PNF firewall which restricts the number of open ports. RSvP services are bound only to GE IP addresses.
- AW Server does not host email or IM clients.
- Prior to commercial release, AW Server has passed several security scans against known vulnerabilities.

**There is no recommendation to install the ClamAV® by default.**

Nevertheless, some customers may have a site security policy that requires antivirus. In this case, follow the procedure below to activate ClamAV® on each AW Server on the site.

Once activated on a system using the parameters described below, ClamAV® provides the following protection:

- Nightly (or manual) scans of vulnerable directories. Real-time scanning is not available as this has serious negative impact on clinical performance.
- Only directories in which malicious file can be inadvertently installed are scanned (if using the parameters in the instructions below). DICOM files are not scanned, as typically these are not susceptible to attack. The scanned directories are:
  - /home/
  - /export/home/
- After set-up, scan logs are located in /export/home/sdc/logfiles.

## A.5.1 Activating ClamAV®

To activate ClamAV® on the server, the network must have:

- Connection to internet
  - HTTP Proxy defined (contact the local Network Administrator for details)
1. Start a Terminal tool and login as **root**.  
See [A.8.1 Accessing the Terminal and login as root on page 589](#).
  2. Edit the /var/spool/cron/root file:  
a. Run crontab:

**crontab -e <Enter>**

### NOTE

By default, the text editor is vi. To use the gedit editor, type the following command before typing the crontab command:

**export EDITOR=gedit <Enter>**

The editor window opens.

- b. Remove the # at the beginning of the following line:

```
# 0 3 * * * /usr/bin/freshclam > /export/home/sdc/logfiles/
clam_scan.log; nice /usr/bin/clamscan -r -l /export/home/sdc/
logfiles/clam_scan.log /home /export/home
```

- c. Save the file and quit the editor.

The newly activated line in the crontab sets the package to scan the listed directories nightly at 03:00. A new logfile (/export/home/sdc/logfiles/clam\_scan.log) is created nightly. Previous logfiles are archived.

3. Change the ClamAV® directory owner:

```
chown clamupdate /var/lib/clamav <Enter>
```

4. Update virus signatures:

- a. Add the Proxy server information to the `freshclam.conf` file:

```
cd /etc <Enter>
```

```
gedit freshclam.conf <Enter> (only available at the KVM)
```

```
vi freshclam.conf <Enter> (available both from the Client PC or FE laptop, and at the KVM)
```

Locate the HTTP proxy parameters above, uncomment (remove the # character) and modify them as the following:

```
HTTPProxyServer n.nnn.nnn.nn
```

```
HTTPProxyPort xx
```

where `n.nnn.nnn.nn` is the IP of the site proxy to use and `xx` is the corresponding port.

I.e: `HTTPProxyServer 3.249.104.45`

```
HTTPProxyPort 88
```

- b. Run `freshclam`:

```
freshclam <Enter>
```

#### **NOTE**

For further details, refer to on-line documentation: <http://www.clamav.net/doc/cvd.html> or the `freshclam.conf` man page (`man freshclam.conf`).

Below is an example message output of a successful `freshclam` update. Warnings can be ignored.

```
ClamAV update process started at Wed Sep 8 12:16:34 2010
```

#### **WARNING**



Can't query current.cvd.clamav.net

#### **WARNING**



Invalid DNS reply. Falling back to HTTP mode.

```
Connecting via 3.249.104.45
```

```
Reading CVD header (main.cvd): OK (IMS)
```

```
main.cvd is up to date (version: 52, sigs: 704727, f-level: 44, builder: sven)
```

```
Connecting via 3.249.104.45
```

```
Reading CVD header (daily.cvd): OK
```

```
Downloading daily-11842.cdiff [100%]
```

```
Downloading daily-11843.cdiff [100%]
```

```
Downloading daily-11844.cdiff [100%]
daily.cld updated (version: 11844, sigs: 121016, f-level: 53, builder:
arnaud)
```

**WARNING**

Your ClamAV installation is OUTDATED!

**WARNING**

Current functionality level = 51, recommended = 53

DON'T PANIC! Read <http://www.clamav.net/support/faq>

Connecting via 3.249.104.45

Reading CVD header (bytecode.cvd): OK (IMS)

bytecode.cvd is up to date (version: 40, sigs: 9, f-level: 53, builder: edwin)

Database updated (825752 signatures) from database.clamav.net

**WARNING**

Clamd was NOT notified: Can't connect to clamd through /var/lib/clamav/

clamd-socket connect(): No such file or directory

## A.5.2 Testing ClamAV®

- To test that ClamAV® is working, execute the command:

```
clamscan -r /export/home/sdc/logfiles <Enter>
```

This performs a test scan on the logfiles directory, directing output messages to the command window.

## A.5.3 Running ClamAV® manually

- To run ClamAV® manually locally on the AW Server, or via a remote login (telnet session), use a command similar to the line added to the crontab.

Example of directing output to a log file:

```
/usr/bin/freshclam > /export/home/sdc/logfiles/clam_manual_scan.log ; \
nice clamscan -r -l /export/home/sdc/logfiles/clam_scan.log <Enter>
```

Adapt the directories scanned and the output according to specific needs.

## A.5.4 Checking ClamAV® status and logs

- 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
```

## **A.5.5 Managing an infection**

If a virus is identified or infected files are detected during a manual scan or in a log file:

1. Check other systems on site to have a full picture of the problem.
2. Contact the GEHC OLC before cleaning the system (removal or quarantine of infected files). Never attempt remedial action without first seeking advice. There is a risk that the system could become unstable, and/or client data could be lost.
3. Recommend to the customer that, although the risk from a virus on a Linux-based system is very low, they should backup images stored on affected system(s).
4. Backup the AW Server's configuration data.

See [2.20 Job Card IST012 - Virtual Servers Cluster Configuration](#) on page 244 for details.

5. Remove the ClamAV® log files.

#### **NOTICE**

If ClamAV® has to be deactivated, perform the above procedure prior to deactivation.

## **A.6 Software Loading Through iLO**

### **A.6.1 Foreword**

Some sites do not authorize to access the servers room once the system has been installed, unless there is a hardware failure. These sites request that the GEHC FE proceeds with any maintenance action such as Software loading, remotely from the Client PC, or from the FE laptop.

OS and AWS platform software can be loaded remotely using the iLO service processor, by "mapping" and using the Client PC media drive.

Applications loading can also be done through iLO, from their media via the Version Management feature of the Service Tools.

See [2.17 Job Card IST009 - External Application\(s\) Installation](#) on page 172 for details.

## A.6.1.1 Pre-conditions

### NOTICE

Remote software loading is dependent of the Network traffic. This might be an issue on certain sites and/or at certain time of the day, when the network traffic is heavy.

- The Client PC or FE laptop should be reserved for this task, that is to say you should avoid running other tasks or programs such as mail, to save all necessary CPU resources for the purpose of remote software loading through the Client PC media drive.
- Preferably turn off automatic features like screen saver or automatic backup. The whole of CPU resources of the Client PC should be dedicated to loading software from the media drive.

## A.6.1.2 Before you start

- Make sure your customer has saved all patient data. Patient data is normally preserved during software load from cold, but it is safe to have all patient data present on the AW server stored on another system, preferably the archiving system of the site.
- Proceed with the AW Server system backup. See [3.10 Job Card UPG001 - Software Upgrade](#) on page 495.
- Write down all necessary data for reinstalling the network and UPS parameters:
  - hostname(s)
  - IP address
  - Netmask/Network prefix
  - Default Gateway
  - Internet routers (if applicable)
  - UPS configuration

## A.6.2 Starting the software load

All the following steps to be done at the Client PC or FE laptop.

## A.6.2.1 Software load preparation with iLO 5

1. In a first navigator window, login into the Service Tools as **service**.
2. Go to the **Maintenance** mode and make sure no users are currently connected.  
If users are connected, make the necessary arrangement to have them properly disconnected, allowing a grace delay before shutdown. Refer to [3.10 Job Card UPG001 - Software Upgrade](#) on page 495 for details.
3. Insert the software media into the Client PC (or FE laptop).
4. In a second navigator window, login into the iLO Service processor ([http://<iLO\\_IP\\_address>](http://<iLO_IP_address>)) as **root** through the Client PC (or FE laptop).
5. Select **Security > Access Settings**.

The *Security - Access Settings* page appears.

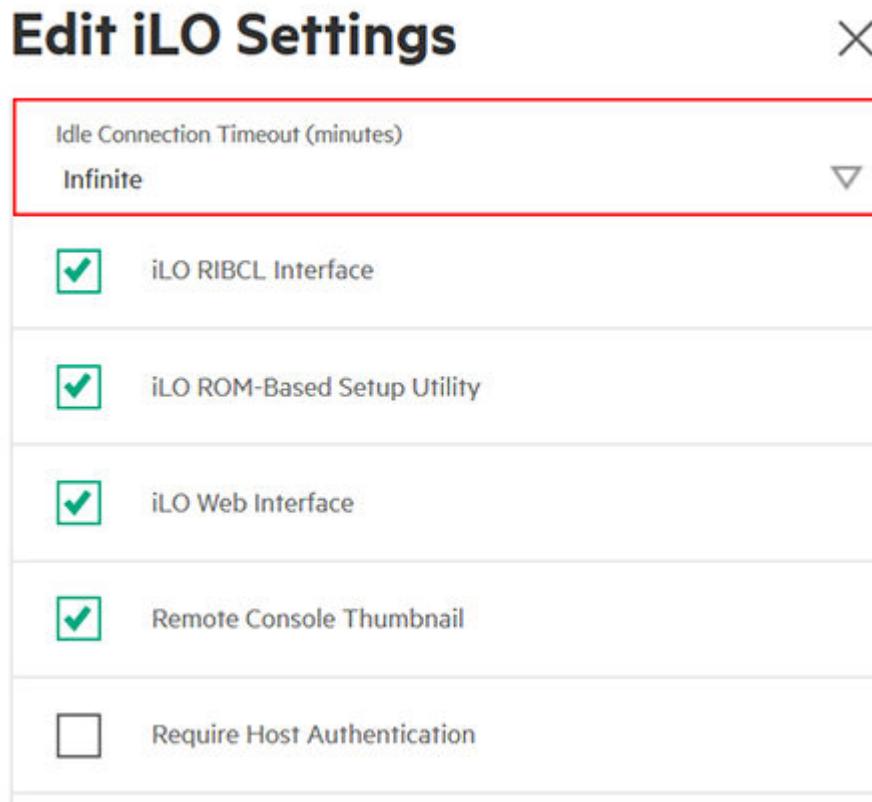
6. Scroll down to *iLO* and click on the **Edit** icon.

*iLO*



|                                               |                                   |
|-----------------------------------------------|-----------------------------------|
| <b>Idle Connection Timeout (minutes)</b>      | 30                                |
| <b>iLO Functionality</b>                      | Enabled                           |
| <b>iLO RIBCL Interface</b>                    | Enabled                           |
| <b>iLO ROM-Based Setup Utility</b>            | Enabled                           |
| <b>iLO Web Interface</b>                      | Enabled                           |
| <b>Remote Console Thumbnail</b>               | Enabled                           |
| <b>Require Host Authentication</b>            | Disabled                          |
| <b>Require Login for iLO RBSU</b>             | Disabled                          |
| <b>Serial Command Line Interface Speed</b>    | 9600                              |
| <b>Serial Command Line Interface Status</b>   | Enabled - Authentication Required |
| <b>Show iLO IP during POST</b>                | Enabled                           |
| <b>Show Server Health on External Monitor</b> | Enabled                           |
| <b>VGA Port Detect Override</b>               | Enabled                           |
| <b>Virtual NIC</b>                            | Disabled                          |

- In order not to be disconnected from the Service Processor during the software load process, change the **Idle connection timeout** value from the default value (**30mn**) to **Infinite** and click on **OK** at the bottom of the page to save the change.



- Click on **Remote Console & Media**.

The *Remote Console & Media - iLO Integrated Remote Console* page appears.

- Click on the **.NET Console** button.

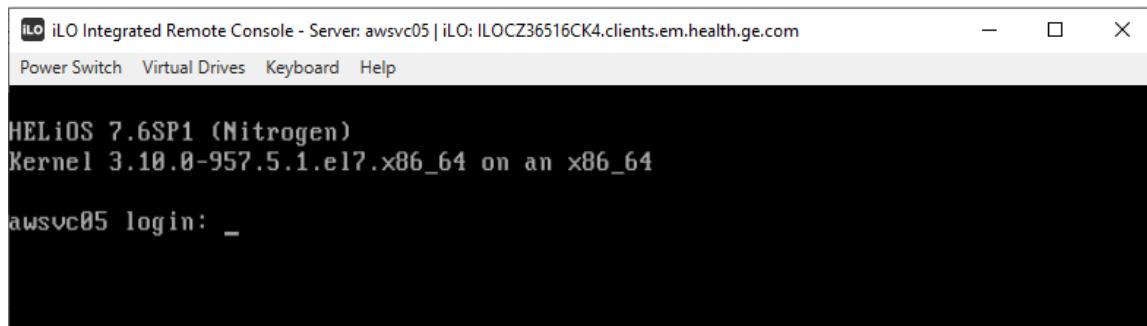
#### **NOTE**

You may have to accept the download and installation of the Microsoft.NET piece of software as described in the *Remote Console & Media - iLO Integrated Remote Console* page.

A license key is necessary to use the iLO Integrated Remote Console. This license is factory installed for GEHC products at HP manufacturing.

In case the iLO Integrated Remote Console would not start, refer to AW Server 3.2 Advanced Service Manual 5771771-8EN at chapter 2, section 2.7. Check if the license is present, and install it if not.

The *iLO Integrated Remote Console* opens and displays the current status of the AW Server.



#### **NOTE**

If the steps that are described here are failing and you cannot successfully use the iLO Integrated Remote Console, use instead the Java Integrated Remote Console.

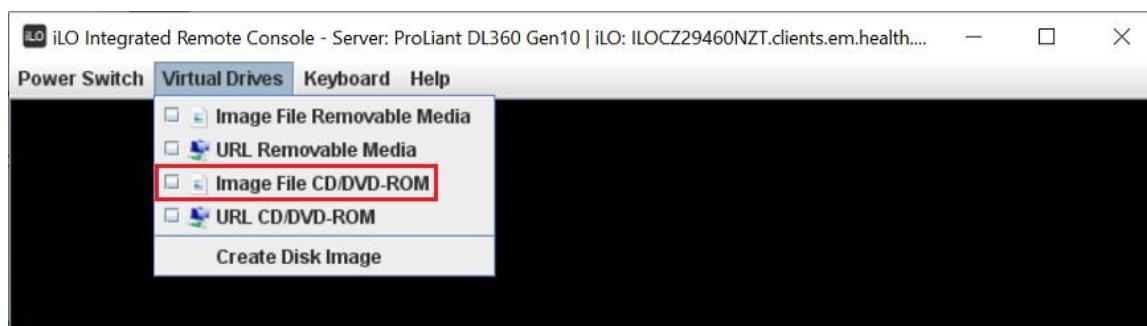
#### **NOTE**

When using the iLO Console Redirection, according to your local PC keyboard mapping, in order to use typing the commands, it may be necessary to setup the Client PC (or FE laptop) locales variable for keyboard.

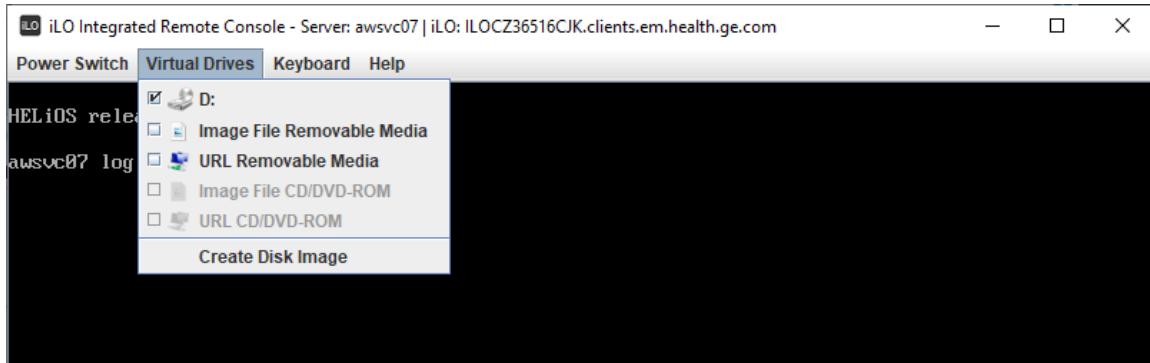
(I.e: type :**loadkeys fr <Enter>** for French kbd mapping).

Variables will reset to us at the next reboot.

10. For a USB media, map the iso file to the CD/DVD drive:
  - a. Click on **Virtual Drives** and select **Image File CD/DVD-ROM**.
  - b. Locate the iso file and select it.



11. For a DVD media, map the Client PC media drive by clicking on **Virtual Drives** and select drive **D:** (or **E:** if any).



You are now ready for remote software loading.

Refer to chapter 3 for more details on the software Load From cold steps.

## A.6.2.2 Software load preparation with iLO 4, iLO 3

### NOTE

The following procedure details the steps for the **iLO 4** (it is similar for **iLO 3**).

1. In a first navigator window, login into the Service Tools as **service**.
2. Go to the **Maintenance** mode and make sure no users are currently connected.  
If users are connected, make the necessary arrangement to have them properly disconnected, allowing a grace delay before shutdown. Refer to [3.10 Job Card UPG001 - Software Upgrade on page 495](#) for details.
3. Insert the software media into the Client PC (or FE laptop).
4. In a second navigator window, login into the iLO Service processor ([http://<iLO\\_IP\\_address>](http://<iLO_IP_address>)) as **root** through the Client PC (or FE laptop).

The *iLO Overview* page appears.

The screenshot shows the "iLO Overview" page for an iLO 4 ProLiant DL360 Gen9 server. The left sidebar has a tree view with "Information" expanded, showing "Overview" (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 content area has two sections: "Information" and "Status". Under "Information", it lists: Server Name (awsvc05), Product Name (ProLiant DL360 Gen9), UUID (32353537-3835-5A43-3336-353136434B34), Server Serial Number (CZ36516CK4), Product ID (755258-B21), System ROM (P89 v2.30 (09/13/2016)), System ROM Date (09/13/2016), Backup System ROM (09/13/2016), Integrated Remote Console (.NET, Java Web Start, Java Applet), License Type (iLO Advanced), iLO Firmware Version (2.50 Sep 23 2016), IP Address (3.249.12.61), Link-Local IPv6 Address (FE80::E207:1BFF:FEEC:AD24), and iLO Hostname (ILOCZ36516CK4.clients.em.health.ge.com). Under "Status", it shows: System Health (OK), Server Power (ON), UID Indicator (UID OFF), TPM Status (Not Present), SD-Card Status (Not Present), and iLO Date/Time (Mon Aug 26 17:57:10 2019). Below this is a "Connection to HPE" section with a warning icon and the text "Not registered". The right side of the page shows "Active Sessions" with two entries: "User" (Local User: root) and "IP Address" (3.249.170.67), with "Source" (HTTPS) listed below. The top right corner shows "Local U" and "iLO Hostname: ILOCZ36516CK4.clients.em.health.ge.com".

5. Expand the **Administration** menu and select **Access Settings**.

The *Access Settings* page appears.

**Access Settings**

**Notes**

- Applying new Port or iLO Functionality settings will require a restart of iLO and terminate this browser connection. It may take several minutes before you can reestablish a connection.
- Changes to the Idle Connection Timeout may not take place immediately in current user sessions but will be immediately enforced in all new sessions.

| Service                   | Access Options |
|---------------------------|----------------|
| Secure Shell (SSH) Access | Enabled        |
| Secure Shell (SSH) Port   | 22             |
| Remote Console Port       | 17990          |
| Web Server Non-SSL Port   | 80             |
| Web Server SSL Port       | 443            |
| Virtual Media Port        | 17988          |
| SNMP Access               | Enabled        |
| SNMP Port                 | 161            |
| SNMP Trap Port            | 162            |
| IPMI/DCMI over LAN Access | Enabled        |
| IPMI/DCMI over LAN Port   | 623            |

**Access Options**

- Idle Connection Timeout (minutes): Infinite (highlighted with a red box)
- iLO Functionality: Enabled
- iLO ROM-Based Setup Utility: Enabled
- Require Login for ILO RBSU: Disabled
- Show iLO IP during POST: Enabled
- Serial Command Line Interface Status: Enabled - Authentication Required
- Serial Command Line Interface Speed: 9600
- Virtual Serial Port Log: Disabled
- Minimum Password Length: 8
- Server Name: awsvc07
- Server FQDN / IP Address:
- Authentication Failure Logging: Enabled - Every 3rd Failure
- Authentication Failure Delay Time: 10 seconds
- Authentication Failures Before Delay: 1 Failure causes no delay

**Apply**

- In order not to be disconnected from the Service Processor during the software load process, change the **Idle connection timeout** value from the default value (**30mn**) to **Infinite** and click on **Apply** to save the change.
- Expand the **Remote Console** menu and select **Remote Console**.

The **Remote Console - iLO Integrated Remote Console** page appears.

**Remote Console - iLO Integrated Remote Console**

**.NET Integrated Remote Console (.NET IRC)**

The browser indicates that you have a supported .NET Framework version.

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 supports the following versions of the .NET Framework: 3.5 (Full), 4.0 (Full), 4.5 and 4.6.

**Launch**

**Java Integrated Remote Console (Java IRC)**

The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java Web Start console or applet-based console. Hewlett Packard Enterprise recommends using the latest version of the Java™ Runtime Environment. This version of iLO was tested with JRE version 8 update 65.

Note: On systems with OpenJDK, you must use the Java Applet option with a browser (such as FireFox) that supports a Java plug-in.

**Web Start** **Applet**

**HPE iLO Mobile App**

The HPE iLO Mobile application provides access to the remote console of your HPE server from your mobile device. The mobile app interacts directly with the iLO processor on HPE servers, providing total control of the server at all times as long as the server is plugged in. You can troubleshoot problems and perform software deployments from almost anywhere.

Download, Connect, Manage! Get started today.  
[www.hpe.com/info/iol/mobileapp](http://www.hpe.com/info/iol/mobileapp)

**Learn More**

- Click on the **Launch** button.

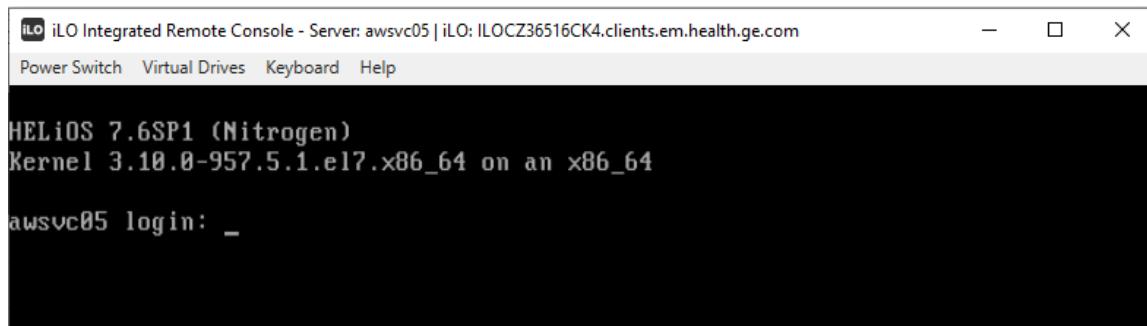
#### NOTE

For the iLO 3 or the iLO 4 service processor, you may have to accept the download and installation of the Microsoft.NET piece of software as described in the *Remote Console - iLO Integrated Remote Console* page.

A license key is necessary to use the iLO Integrated Remote Console. This license is factory installed for GEHC products at HP manufacturing.

In case the iLO Integrated Remote Console would not start, refer to AW Server 3.2 Advanced Service Manual 5771771-8EN at chapter 2, section 2.7. Check if the license is present, and install it if not.

The *iLO Integrated Remote Console* opens and displays the current status of the AW Server.



#### **NOTE**

If the steps that are described here are failing and you cannot successfully use the iLO Integrated Remote Console, use instead the Java Integrated Remote Console.

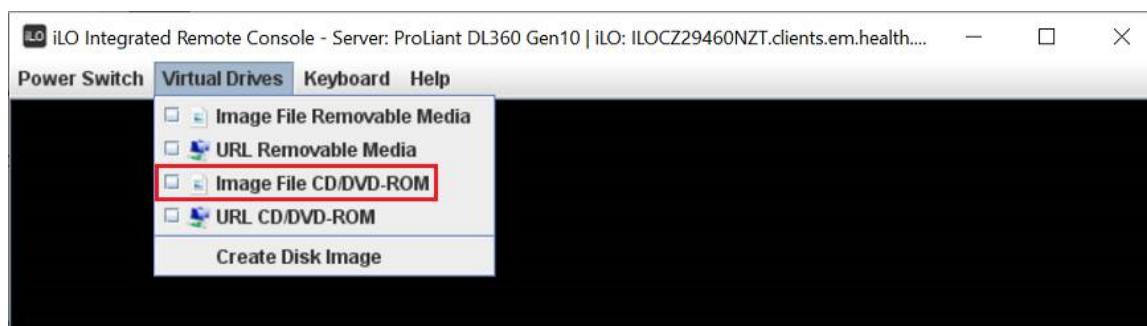
#### **NOTE**

When using the iLO Console Redirection, according to your local PC keyboard mapping, in order to use typing the commands, it may be necessary to setup the Client PC (or FE laptop) locales variable for keyboard.

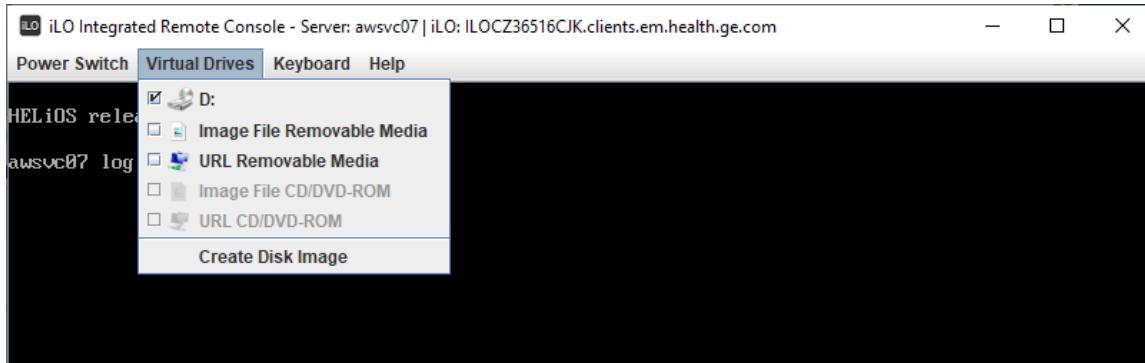
(I.e: type :**loadkeys fr <Enter>** for French kbd mapping).

Variables will reset to us at the next reboot.

9. For a USB media, map the iso file to the CD/DVD drive:
  - a. Click on **Virtual Drives** and select **Image File CD/DVD-ROM**.
  - b. Locate the iso file and select it.



- For a DVD media, map the Client PC media drive by clicking on **Virtual Drives** and select drive **D:** (or **E:** if any).



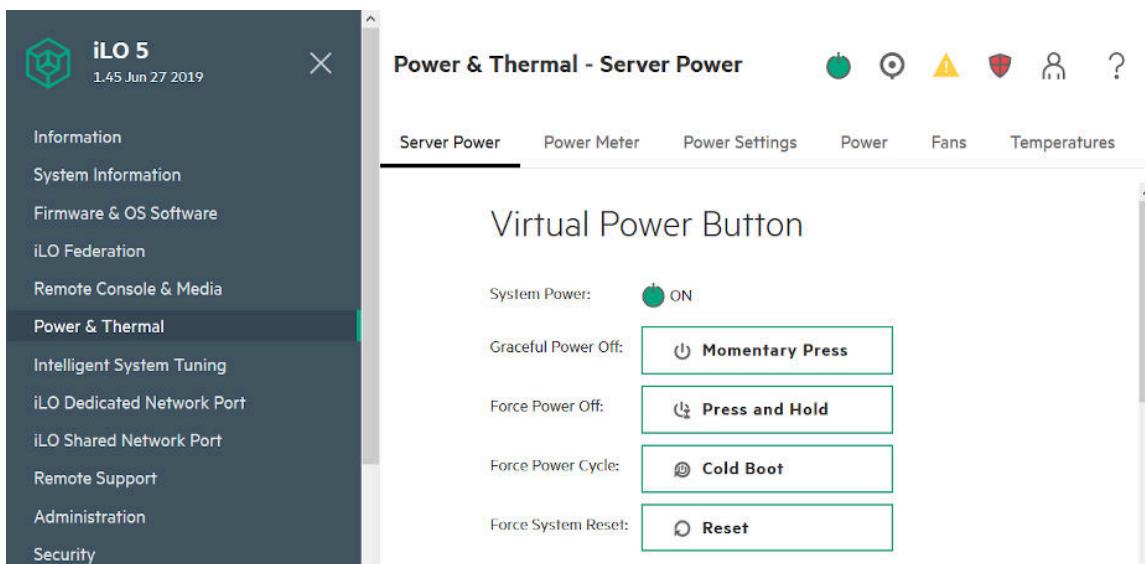
You are now ready for remote software loading.

Refer to chapter 3 for more details on the software Load From cold steps.

### A.6.2.3 Server reboot

This procedure details the steps for iLO 5 (it is similar for iLO 4, iLO 3).

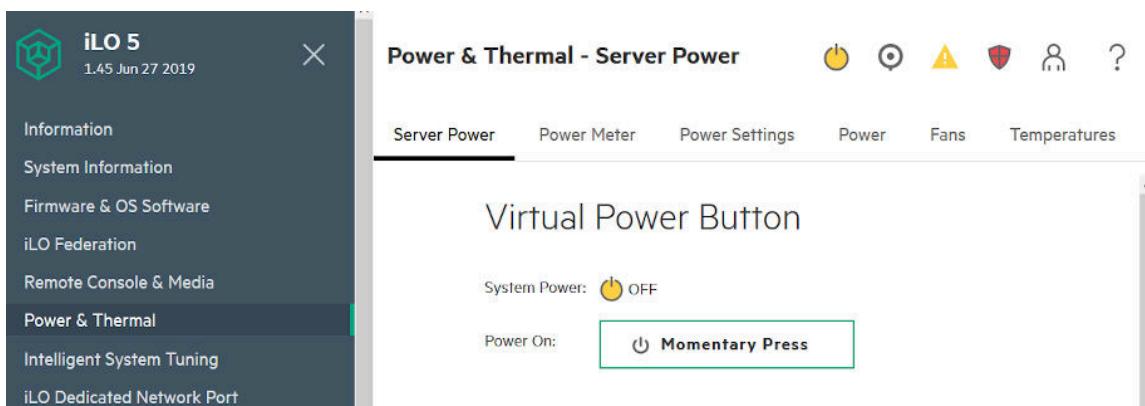
- Click on **Power & Thermal**, then select **Server Power**.



- To shutdown the AW server, click on the **Momentary Press** button.

- Click on **OK** to acknowledge the confirmation message.

After a few seconds, the **System Power** turns to OFF.



4. To restart the AW server, click on the **Momentary Press** button.
5. Click on **OK** to acknowledge the confirmation message.

After a few seconds, the **System Power** turns to ON.

6. Be prepared at the Console to select the boot from AW Server 3.2 media (**Install AW Server 3.2 (vS7)**). In the other case, the system would boot from the hard disk. If this is the case, type **reboot** at the console and make sure you are ready to select Boot from media.

Stay around during the whole load process time in order to make sure the process will not be interrupted for too long time and to avoid losing connection with the iLO, Console redirection and the virtual drive.

#### A.6.2.4 Load From cold steps

- Proceed with the Load From Cold steps (OS + AWS software). Refer to [3.10 Job Card UPG001 - Software Upgrade on page 495](#) for detailed instructions.
- When done, proceed with network and time zone setup, then restore the UPS configuration (if applicable), and install the Applications.

#### A.6.2.5 Applications loading steps

Refer to [2.17 Job Card IST009 - External Application\(s\) Installation on page 172](#) for details.

#### A.6.2.6 Final step

- When you have completed the software Load steps you may want to change the Idle connection timeout value back to the **30 mn** default value.

### A.7 SNMP setup in the iLO service processor

#### NOTE

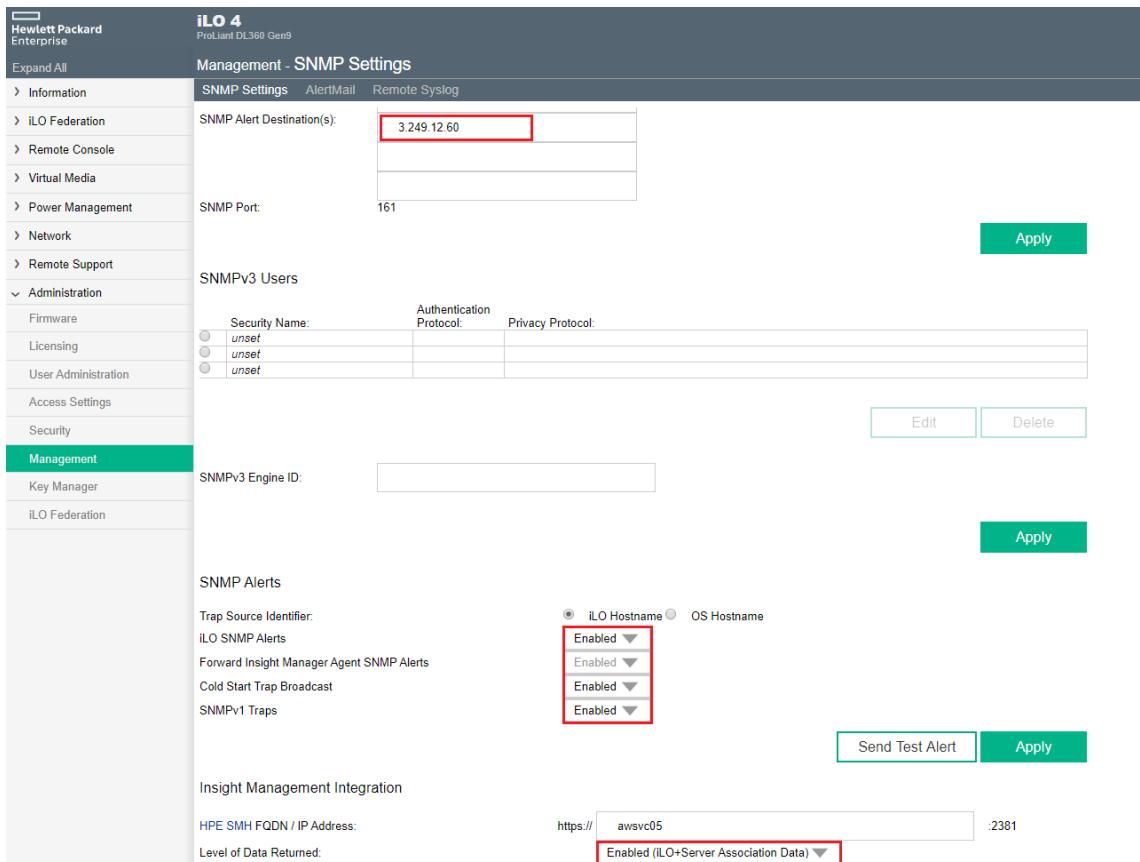
If the Secured for RMF mode is planned to be activated, then do not perform this procedure, keep SNMP in **Disabled** state. SNMP feature is not supported in RMF mode

1. At the Client PC or FE laptop, open a browser (Firefox or Internet Explorer) and type in the AW Server's iLO Service processor IP address.

I.e: <http://3.249.15.25>

2. When the login page loads appears, login as **root**.
3. When the iLO page appears, select **Administration** tab, then click on **Management** tab (see examples below).

Example: iLO 4 (it is similar for iLO 3)



4. Enable / check all Alert trap types are enabled.

HP Insight Manager may not be enabled as HP Insight option is not part of the product offering for GEHC.

5. Make sure that Level of data returned is set to: **Enabled (iLO + Server Association Data)**.

6. In **SNMP Alert Destination**, enter:
  - the site's SNMP server IP address if there is any,
  - or the AW Server IP address.

#### **NOTE**

If the site has an SNMP server, and would like to use it to receive traps, enter its address in the **SNMP Alert Destination** field. Consult the Customer IT Admin to get the IP address of this server.

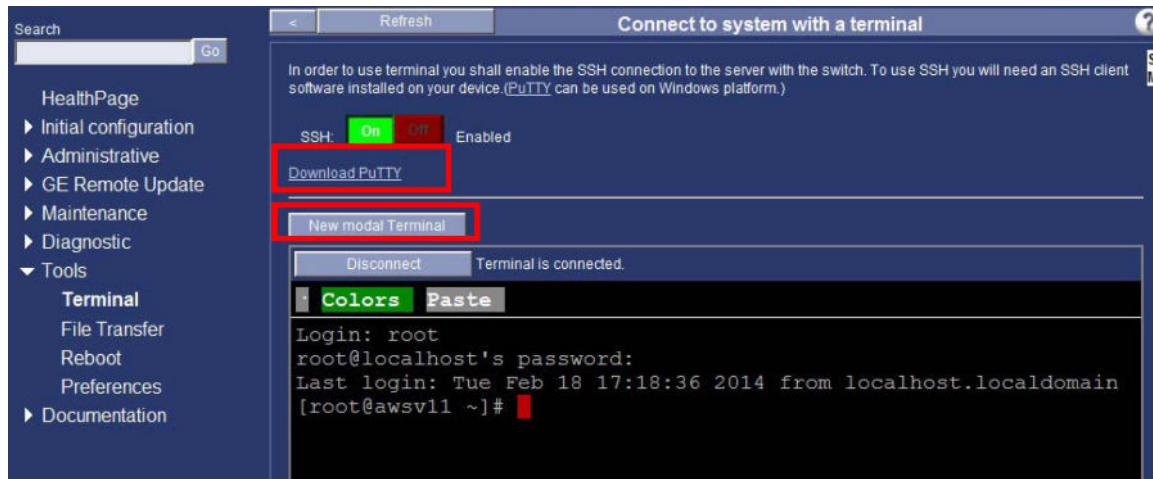
7. Click on **Apply** to save.
8. To send a test alert to the setup destination logfiles, click on **Send Test Alert**.
9. Launch the Terminal from the **Service Tools > Tools** and check the `/var/log/snmptraps.log` file.
10. Logout from the iLO Service processor by clicking on the **Logout** button.

## A.8 Useful Commands and Tools

### A.8.1 Accessing the Terminal and login as root

- Login at the Server's KVM (Keyboard, Video-monitor, Mouse) as **root**
- >>> OR

- From the **Tools** menu, open the **New Modal Terminal**, that allows keeping the login active when moving forward to other Service tools, and back to Terminal:



- Click on the **Connect** button
- Login as **root**

You may also download the PuTTY Terminal (to be used locally only) from the **Download PuTTY** link provided in the Service Tools interface.

## A.8.2 Shutting down or rebooting the server

### NOTICE

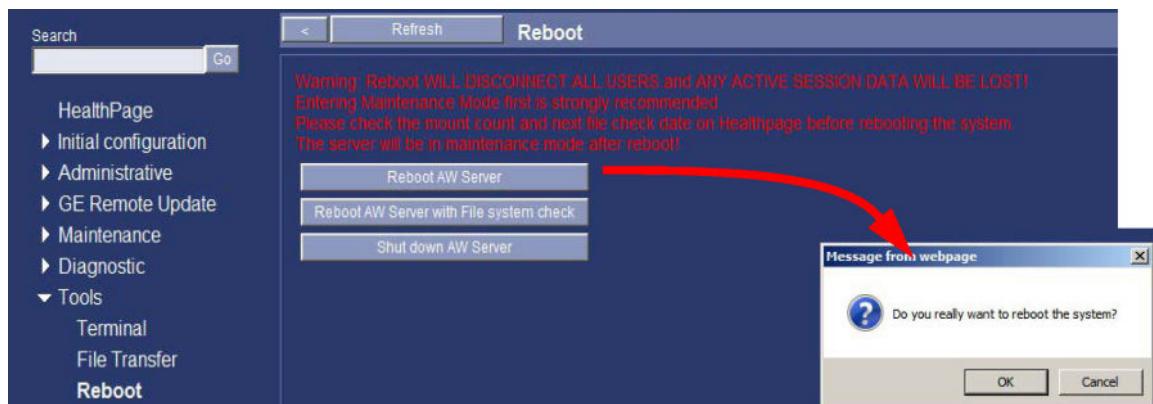
**Always use the shutdown command with precaution.** If your system is close to the maximum mount count or passed the 6 month delay, shutting down the server may trigger the Filesystem check at next reboot and introduce several hours delay before the server becomes available again. Refer to [A.9 Filesystem Check on page 595](#) for details.

### NOTICE

**Always consider checking** if there are users connected, and send a warning message allowing a grace delay of a few minutes prior to shutdown. Refer to [A.4 Maintenance Mode on page 571](#) - Maintenance mode.

### A.8.2.1 Through the Service Tools menu

- From the Tools menu, click on the **Reboot** sub-menu:



- Select the appropriate reboot or shutdown tool and acknowledge the confirmation message that pops up. The available tools are available via the following buttons:
  - **Reboot AW Server**
  - **Reboot AW Server with Filesystem check.** You can force the filesystem check to launch it at the most appropriate moment for the site.
  - **Shutdown AW Server**

### A.8.2.2 Through command lines

TO BE USED CAUTIOUSLY - NEXT REBOOT TIME MAY LAST SEVERAL HOURS

- To reboot the server, type in:

**reboot <Enter>**

- To shutdown the server, type in:

**shutdown -h 0 <Enter>**

- To shutdown the server, and send a message to the connected clients:, type in:

**shutAWSdown <Enter>**

- To shutdown the server, and force *Filesystem check* at reboot, type in:

**touch /forcefsck <Enter>**

**reboot <Enter>**

### A.8.3 Checking the routing table

- To check the routing table, type in:

**ip route <Enter>**

### A.8.4 Checking the Network settings

- To check the network settings, type in:

**ip addr <Enter>**

### A.8.5 Checking the AWS configuration

- To check the AWS configuration, type in:

**/usr/local/bin/conf <Enter>**

**/usr/local/bin/conf -long <Enter>** (gives additional configuration information)

- To check the AWS release, type in:

**cat /etc/aweconfig <Enter>**

### A.8.6 Checking the OS release

- To check the OS release, type in:

**cat /etc/aweos <Enter>**

### A.8.7 Launching the Internet Navigator from the Server's KVM

The AW server is up and running.

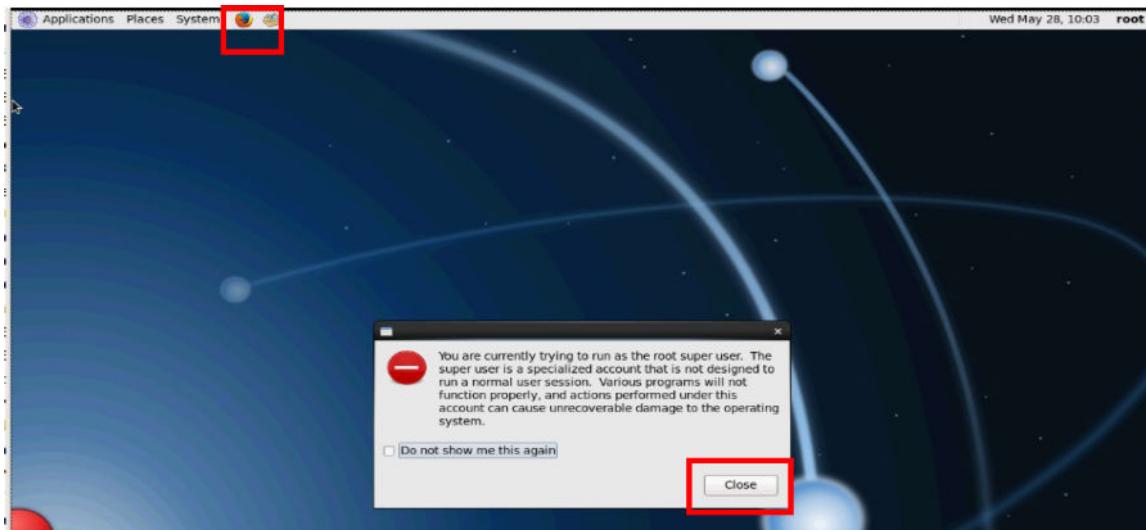
1. At the Server's KVM (Keyboard, Monitor and Mouse), login as **root**.

2. Launch the Xserver to start the graphical mode.

**startx <Enter>**

The message Current resolution is not supported. Reverting to best display setting. may appear. This message can be acknowledged by pressing any button on the KVM screen.

3. When the graphical mode starts, acknowledge the warning message by ticking the **Do not show me this again** checkbox and clicking on the **Close** button. Then, click on the Firefox icon located at the upper left of the screen.



The Mozilla Firefox navigator page opens.



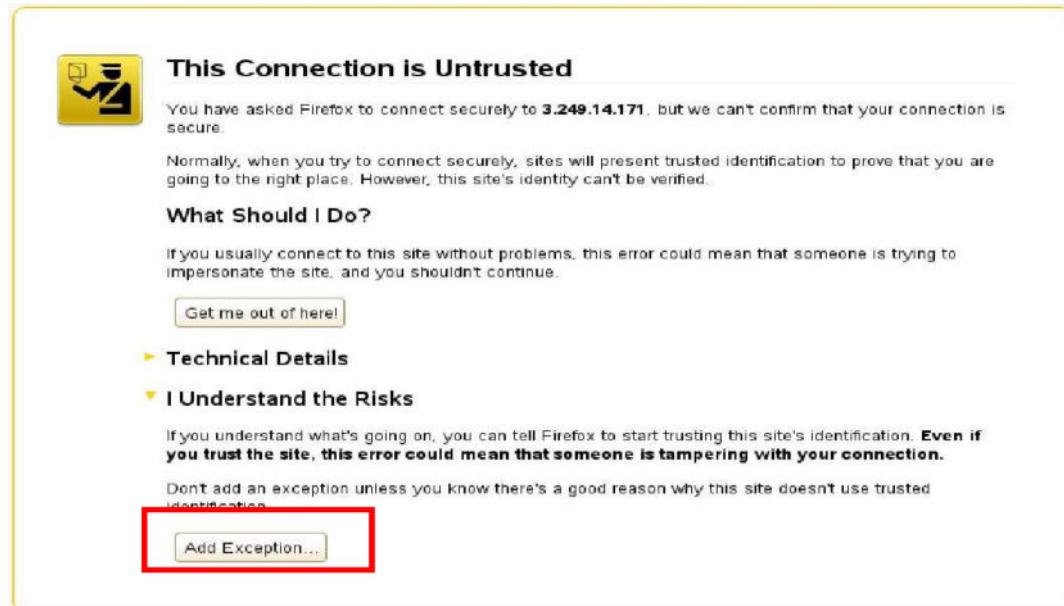
4. Connect to the Server by typing its IP address or its iLO/iLOM service processor address:

[http://<IP\\_address\\_server>](http://<IP_address_server>) I.e: <http://3.249.12.114>

### NOTE

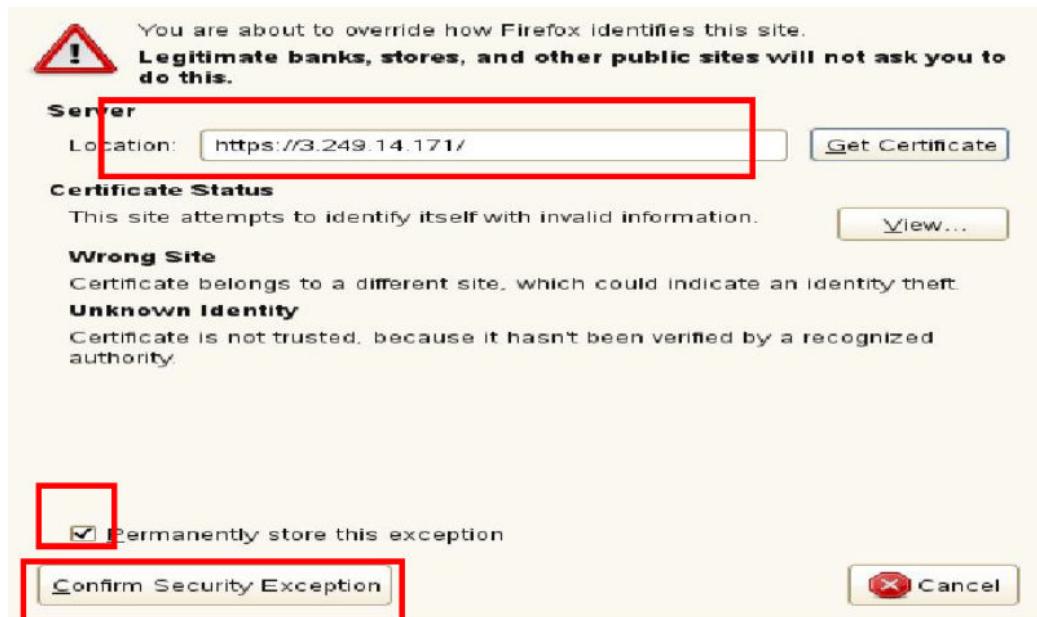
Instead of entering the IP address, it is possible to enter <http://localhost/> since Mozilla Firefox is running directly on the server. It is interesting because Service Tools can be accessed even when IP address is not configured or not working.

If you start Mozilla Firefox in secure mode (<https://>), the following page appears:



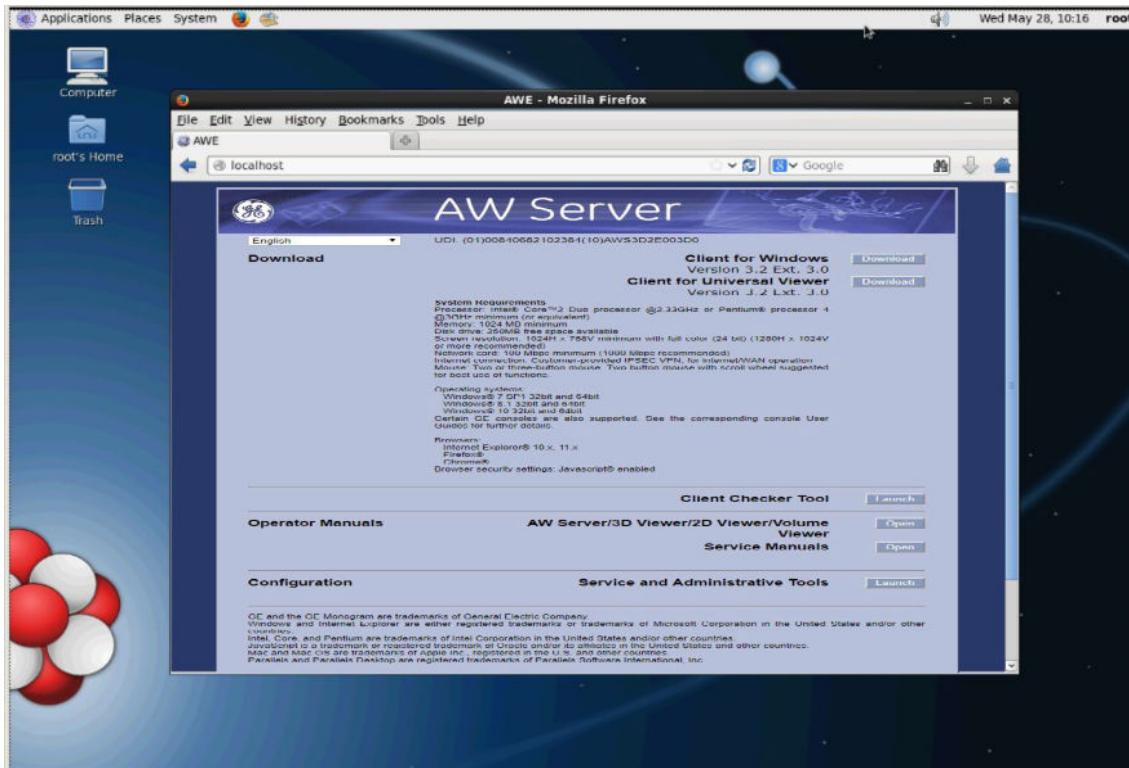
- Click on **I Understand the Risks** then on **Add Exception...**

The following window appears:

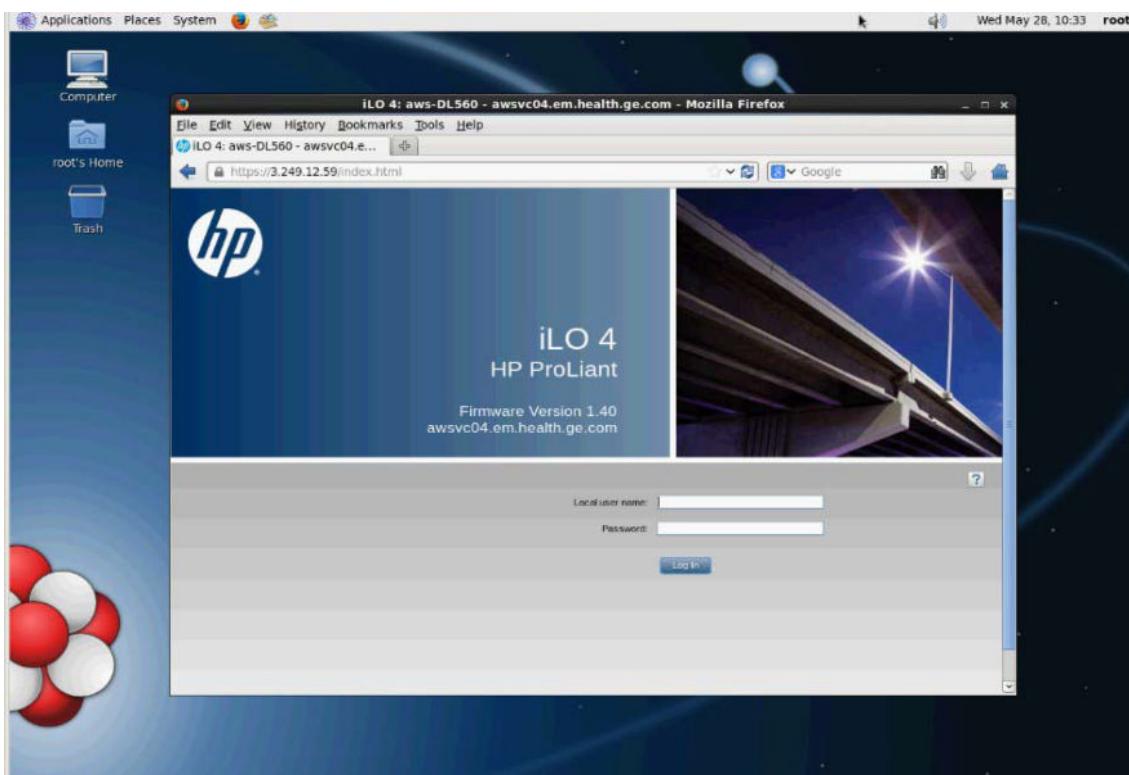


- Check that the IP address of the AW Server is correct.
- Make sure that the **Permanently store this exception** checkbox is ticked.
- Click on the **Confirm Security Exception** button.

If you typed the AW Server IP address or localhost, the AW Server login interface appears:



If you typed the iLO IP address, the iLO (iLO 4 in our example) login page appears:



## A.8.8 DNS server(s) setup - Alternate method

In case the site's DNS server(s) have not been set up during the early installation steps (see [2.13 Job Card IST005 - Network and Time Configuration on page 127](#)), for example if the information was not available at that time, you can configure it (them) through the Service Tools at a later moment.

DNS server(s) is (are) mandatory if your AW Server shall be integrated with the PACS and/or if your site has EA3 Users authentication system.

## A.8.8.1 Enter the Maintenance mode

To setup the DNS server(s), it is necessary to place the AW Server in the Maintenance mode.

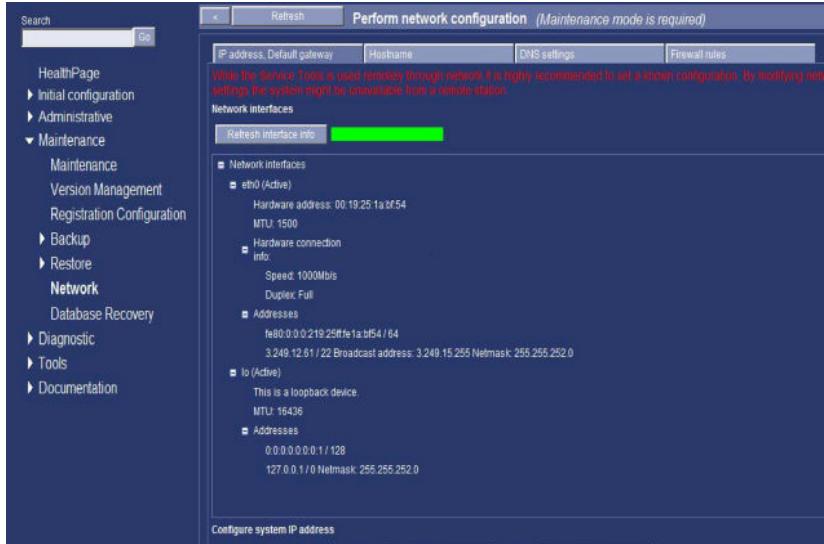
1. Click on **Maintenance** menu then select **Maintenance**.
2. Proceed with the preliminary steps prior to place the system in Maintenance mode.

Refer to [A.4 Maintenance Mode on page 571](#) for details.

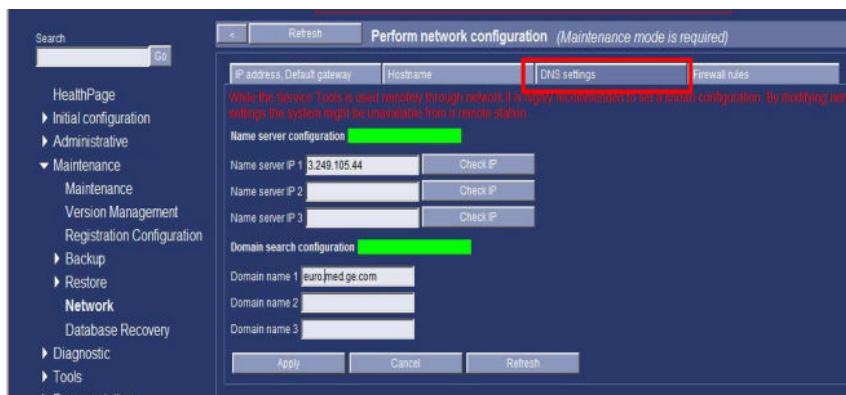
## A.8.8.2 Setup the DNS server(s)

1. Click on **Network**.

The *Perform network configuration* panel appears.



2. Click on **DNS settings**.



3. Enter the DNS server(s) IP address(es) and the Domain name(s).
4. Click on **Check IP** to verify that the DNS server Host(s) is (are) alive.
5. Click on **Apply**.

## A.9 Filesystem Check

## A.9.1 Filesystem Check feature description

### NOTE

The filesystem check impact is less significant for full, Seamless or DICOM Direct Connect integration, as there is no Image Database partition. The image partition used to temporarily store the images processed on AW Server before sending them to the PACS is small, therefore the filesystem check time is reduced to a few minutes.

The AW server is programmed to regularly run a Filesystem check upon reboot after a certain number of boot-up: around 30 - Note that this value can be set differently.

This figure is available in the **System Configuration** section of the **HealthPage**:

When the mouse is pointed over the Mount count, it provides a short description about the meaning of the field, and also mentions the rules for its coloring (i.e: yellow means less than 5 restarts allowed before filesystem check will be started).

|                                                 |                                               |  |
|-------------------------------------------------|-----------------------------------------------|--|
| OSU                                             | 100                                           |  |
| REF                                             | 57                                            |  |
| LOT                                             | AW                                            |  |
| Uptime                                          | 23:                                           |  |
| Region / Timezone                               | EU                                            |  |
| Memory Total / Free                             | 9850 / 9500                                   |  |
| OS Disk Space Total / Free                      | 110 (GB) / 94 (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) / 18 (GB)                             |  |
| AWeDIM Disk Space Total / Free                  | 68 (GB) / 55 (GB)                             |  |
| Network Queue Status                            | In progress: 0 Pending: 0 Paused: 0 Failed: 0 |  |
| Auto Delete (High / Low)                        | -                                             |  |
| Delete option for worklist browser              | Off                                           |  |
| Image partition mount count<br>(Current / Max.) | 3/30                                          |  |
| Signer certificate expiration date              | Sun 01 Oct 2026 10:41:35 AM CEST              |  |

### NOTICE

The filesystem Check (fsck) 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.

### NOTICE

**Once the filesystem check is started there is no option to skip it. If the system is rebooted during filesystem check, the filesystem can be damaged.**

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 the mount count for System, and the mount count for 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, therefore the mount count is not effective for them.

## A.9.2 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 boot up sequence time (depending on the number of images stored on the hard disks).

## A.9.3 Solutions to minimize the impact

### 1. Check when the next Filesystem check is programmed.

Refer to the System configuration section of the HealthPage as shown in section 7-1

#### **NOTE**

Alternate method to check when the next Filesystem check is programmed:

- Open the terminal under Service Tools/Tools, login as **root**
- Identify the proper block device corresponding to the images directory.

**df -k <Enter>**

I.e: /dev/xxx.....

/dev/sdb2 xxx xxx xxx xx% /export/home1

Depending on server type, image filesystem can be on sda2 or sdb2.

- Query the file system properties

**tune2fs -l /dev/sdb2 <Enter>** (or /dev/sda2)

I.e: .....

*Mount count: 26*

*Maximum mount count: 28*

*Last checked: Mon May 30 15:29:08 2014*

*Check interval: 15552000 (6 months)*

*Next check after: Sat Nov 29 14:29:08 2014*

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.

So in that case, warn the IT Admin that the Filesystem Check is going to occur soon, so that they can force a check in advance over the next weekend for instance.

### 2. Minimize the impact for the users - Warn the IT admin asap

In order to minimize the impact for the users, the GEHC FE should warn asap the IT admin about this feature and its side effect, and let them know the procedure for forcing the "fsck" launch at the best possible moment - i.e: before a weekend.

### 3. Minimize the impact for GEHC FE

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 to shutdown and reboot 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, prior 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

the Terminal under Service Tools/Utilities 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 boot up sequence and therefore to FE on-site time.

- Reboot the server forcing the filesystem check

**touch /forcefsck <Enter>**

**reboot <Enter>** OR

- Click on the button "**Reboot AW Server with filesystem check**" utility in the Service Tools, under **Tools / Reboot** menu.

Filesystem check can take several hours depending on the number of images stored on the system. You can monitor the progress on the terminal (KVM) in the server room or with the console redirection of the iLO. When *Welcome to Scientific Linux* screen displays, press the **<Esc>** key to view the progress message.

```
Starting udev: [ OK ]
Setting hostname awsvc03: [ OK ]
Setting up Logical Volume Management: No volume groups found [ OK ]
Checking filesystems
/dev/sdb3: clean, 146743/3276800 files, 3179742/13107200 blocks
/dev/sda1 has gone 201 days without being checked, check forced.
/dev/sda1: 18/244320 files (0.0% non-contiguous), 33647/976128 blocks
/dev/sda2 has gone 201 days without being checked, check forced.
/dev/sda2: ===== \ 96.1%
```

After the filesystem check has completed and the AW server has rebooted, the result of the "tune2fs" command should indicate a "Mount count" of 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 (mandatory to maintain system files health), it is possible to postpone the check to a later date if needed.

#### **NOTICE**

These commands shall be run by the GEHC FE, **locally at the KVM of the AW Server**, prior to proceed with the preventive or corrective maintenance tasks, as the "init 2" command will stop all service tools.

- Open a root shell (Terminal: login as **root**)
- 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)

- 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 reports that some processes are using the mount point, you can query the process(es) ID then attempt to stop them:

**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

In this case close the terminal connected to the “import” directory or kill the process as below:

I.e: **kill -9 21386 <Enter>**

Then run the “umount” command again.

- 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/sdb2 <Enter>** (if image filesystem is on /dev/sdb2)

- I.e: change the max mount count to 40

**tune2fs -c 40 /dev/sdb2 <Enter>**

- Invoke 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 unmounted clearly, suggest fsck) !

- Query the file system properties to make sure the modification has been done properly

**tune2fs -l /dev/sdb2 <Enter>**

- Perform reboot

**reboot <Enter>**

Or click on the "Reboot AW Server" button in the Service Tools, under Tools / Reboot menu.

## A.10 Hardware Return Procedure

### A.10.1 Old hardware removal

- De-install the old hardware referring to the Vendor’s service guide instructions (High Tier server) and /or to the old AW Server Installation manual (Low Tier server).

- Refer to AW Server 3.2 Hardware Installation Manual, section *General safety information on rack-mountable products* for general safety information for rack-mountable products and weight lifting posture safety instructions.
- Use the new server hardware packaging to send back the old system.

**NOTE**

When removing a Low Tier server, refer to Low Tier server handling procedure described in the AW Server service manual.

## A.10.2 Old hardware return process

Old hardware equipment shall be returned to the **GEHC Recycling Centers**.

Use the shipping boxes of your new hardware to pack the parts you are returning.

Hardware parts to return are:

- Server box + power cords.
- UPS if applicable
- Monitor + video cable + power cord
- Keyboard + cable and Mouse.
- Network cables

**NOTE**

The addresses below are correct at the time of creation of this manual. Refer to the latest SNAW3044 Service Note to get up-to-date addresses.

**NOTICE**

THE RETURNED EQUIPMENT IS DESTINED FOR RECYCLING! DO NOT RETAIN ANY PART OF IT! MISSING PARTS WILL BE CHARGED!

### A.10.2.1 Return Procedure for Americas

- Use the shipping boxes of new equipment to return old material.

**NOTICE**

Prior to returning the equipment, contact the GE Healthcare Recycling Center to notify them of your equipment shipment. Be sure to write the SO number on the outside of the equipment box so that the Recycling Center can track the returns.

- Return old material and old system Configuration Form located at the beginning of this manual to:

GEHC-RR

Attn: Part Harvest Dept.

7624 South 10 Street

Oak Creek, WI 53154-1912

### A.10.2.2 Return Procedure for ASIA

- Use the shipping boxes of new equipment to return old material.

**NOTE**

Please contact the local Support Engineer of your region, in order to make sure of the right address to return old material.

The following is given for information only, and is subject to change.

Make sure it is still appropriate by contacting your local support.

### A.10.2.3 Return address for Korea

Samsung GE Medical Systems

Mr Jae Young Cho (K0125)

65-1 Sangdaewong-dong, Chungwong-ku

Sungnam-si, Kyunggi-do

KOREA 462-120

### A.10.2.4 Return address for Australia / New Zealand

GE Medical Systems,

Attn: Max Cardew

Unit 6, 13 Lord Street,

Bontany, NSW 2019

Sydney, AUSTRALIA

### A.10.2.5 Return address for GEMS

**NOTE**

Please contact your Regional Service Head Quarters, to get instructions for returning the old Systems hardware.

### A.10.2.6 Return address for East Asia countries

GE Pacific PTE Ltd

Attn: Bryan Heaney

298 Tiong Bahru Road, 15-01/06

Central Plaza, SINGAPORE 168730

### A.10.2.7 Return procedure for other GEHC-Asia countries.

**NOTE**

Please contact your Regional Service Head Quarters, to get instructions for returning the old Systems hardware.

### A.10.2.8 Return Procedure for Europe

- Use the shipping boxes of new equipment to return old material.
- Return old material and old system Configuration Form located at the beginning of this manual to:

Geodis Logistics - Harvest

Bat EVL2 Quai 48 - ZI la pièce de la remise

Route de Corbeil - CD26 - 91090 Lisses - France

- If you are sending from the Region France, ship by the usual Spare Parts return process: (Sernam – Megastore Evry)
- If you are sending from other Regions, use the shuttles to return the Spare Parts. Regional Distribution point or Local depots:

Antwerpen – Frankfurt – London – Madrid – Milano

Athina – Kobenhavn – Istanbul – Kriens – Lisboa – Mockba – Napoli – Stockholm – Wien

Transport costs will be charged by the "Recycling Center". Send the invoice to:

BUC, Compta fournisseur, Ref: Recyclage

## A.11 Physical Servers - Installed Base

This appendix describes the instructions for Installed Based Physical Servers.

### A.11.1 AW Server - Product Description

The IB physical servers:

- HPE ProLiant DL360 Gen9 Server: Low Tier and High Tier.

#### NOTE

The HP ProLiant ML350 G6 Server, HPE ProLiant DL580 G7 Server, HPE ProLiant ML350p Gen8 Server and HPE ProLiant DL560 Gen8 Server are not supported on this AW Server 3.2 release.

#### A.11.1.1 The HPE ProLiant DL360 Gen9 Server low-tier rack-mount version

Based on the HPE ProLiant DL360 Gen9 Server. It supports up to 40,000 slices at a time, depending upon which license is purchased.



#### A.11.1.2 The HPE ProLiant DL360 Gen9 Server high-tier rack-mount version

Based on the HPE ProLiant DL360 Gen9 Server, it supports up to 16,000, 40,000, 80,000 or up to 160,000 slices at a time, depending upon which license is purchased.



## A.11.2 Hardware Installation Verification

## A.11.2.1 HPE ProLiant DL360 Gen9 Server Low Tier and High Tier Server hardware deliverables

- Verify that the Server hardware inventory (provided within server documentation) includes the items below:

- For HPE ProLiant DL360 Gen9 Server High Tier:

| Description                             | Quantity |
|-----------------------------------------|----------|
| HP DL360 chassis                        | 1        |
| 300GB 15K SAS 2.5" HDD                  | 2        |
| 1.8TB 10K SAS 2.5" HDD                  | 6        |
| Internal DVD+/-RW drive                 | 1        |
| Internal RAID controller                | 1        |
| Redundant hot-swappable AC power supply | 2        |
| Tool-less slide rail kit                | 1        |

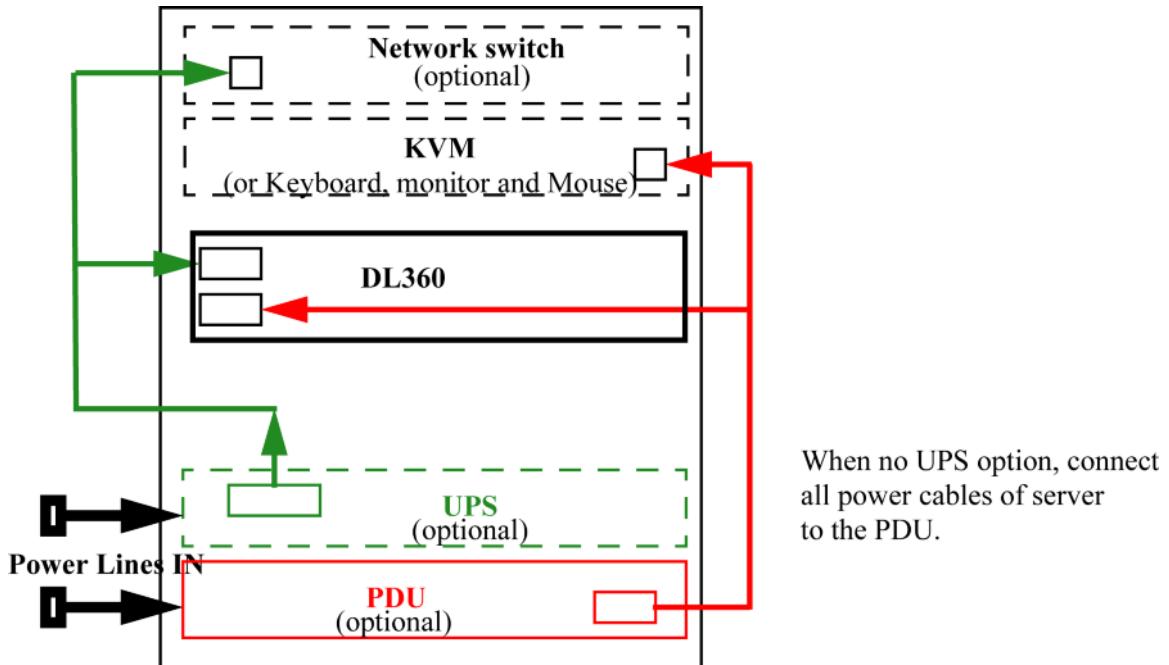
- For HPE ProLiant DL360 Gen9 Server Low Tier:

| Description                             | Quantity |
|-----------------------------------------|----------|
| HP DL360 chassis                        | 1        |
| 300GB 15K SAS 2.5" HDD                  | 2        |
| 600GB 10K SAS 2.5" HDD                  | 6        |
| Internal DVD+/-RW drive                 | 1        |
| Internal RAID controller                | 1        |
| Redundant hot-swappable AC power supply | 2        |
| Tool-less slide rail kit                | 1        |

- Verify that the server slides out and in the rack enclosure easily, and do not bind or cause disconnected cables. This means that the cables, and cable arm harness (if installed) must be dressed and strain-relieved properly.
- Inspect all units to insure that there is no visible chassis damage.
- Verify that the server has two 300GB drives and six 1.8TB drives (High Tier) or six 600GB drives (Low Tier), as shown in the picture below:



- Verify that the Server is connected to a PDU (either data center PDU or rack mount) and/or connected to a UPS (either data center UPS or rack mount).
- If rack mount UPS is installed, verify that UPS is powered on, and that the KVM, Network switch and server are connected to UPS and PDU as shown below.



7.

- HPE ProLiant DL360 Gen9 Server High Tier: Verify that the High Tier server is connected to the network with one cable set on port P1 of the additional Ethernet controller and one cable set on the iLO port.



- HPE ProLiant DL360 Gen9 Server Low Tier: Verify that the Low Tier server is connected to the network with one cable set on port 1 of the Ethernet controller and one cable set on the iLO port , as shown in the picture below:



8. Verify that the KVM (or monitor) is connected to the VGA output and that the keyboard and mouse inputs are connected to the USB port(s).
9. Verify that the UPS auto-shutdown USB input is connected to the one of the USB ports of the server.
10. Apply power to the system. Apply power to the mains inputs of PDU and UPS (if applicable).
  - The UPS utility green LED should blink. The KVM turns on.
  - The Server on/off button LED should be steady yellow.
11. Power up the UPS (if applicable) by pressing on the **On** button.
  - The Network switch option turns on.
  - The UPS Utility LEDs should display steady green as shown.

**Figure A-1 HPE R/T3000 UPS front panel**

12. Power up the server, by pressing on the **Power On** button.



- The Server power on/off button light turns from yellow to green.
  - There will be LED activity on the Server HDDs / SSDs and the LEDs shall be green.
  - The Network 1 LED should be ON (if the network is configured).
  - Hardware initialization sequence takes several minutes to complete. Please be patient. Then after a while, the screen unblanks and will display the HP ProLiant logo and boot up messages.
13. Verify that the following parameters are setup correctly, referring to the AW Server 3.2 Hardware Installation Manual (received/referenced while installing the hardware):
    - a. BIOS parameters (press **<F9>** to enter BIOS setup).

**NOTE**

The BIOS parameters can be checked at any time, without having to reboot the system and enter the BIOS menu as follow:

- In a terminal, login as **root**.
- Type the following command: **/sbin/conrep -s <Enter>**.
- The BIOS parameters are save locally in the file **conrep.dat**, and can be viewed using the command **cat conrep.dat <Enter>** or the command **more conrep.dat <Enter>**.

- b. iLO Service Processor parameters (press **<F8>** to enter iLO setup).
- c. RAID controllers / RAID levels parameters (press **<F8>** to enter RAID setup).
  - P440ar RAID controllers / RAID levels parameters
    - 2 x 300GB HDDs in RAID 1
    - 6 x 600GB HDDs (Low Tier) in RAID 6 OR

- 6 x 1.8TB HDDs (High Tier) in RAID 6

14. Quit the BIOS setup.

Once initialization is complete, the boot sequence will restart and complete as the AW Server has been preloaded by Manufacturing.

**NOTE**

When booting the AW Server, Scientific Linux progress bar is displayed for OS boot. However, details of other operations are not provided. To display the details, hit any of the arrow keys or the <Esc> key. This will display of OS boot messages including filesystem check progress. Hitting any of the arrow keys or the <Esc> key again displays the previous OS boot screen progress bar.



GE HealthCare

[www.gehealthcare.com](http://www.gehealthcare.com)