

GE Healthcare

# MUSE™ Cardiology Information System Service Manual

Software Version 8.0  
2034539-043 D



MUSE Cardiology Information System  
English  
© 2011-2013 General Electric Company.  
All Rights Reserved.

## Publication Information

The information in this manual only applies to MUSE™ Cardiology Information System Version 8.0. It does not apply to earlier product versions. Due to continuing product innovation, specifications in this manual are subject to change without notice.

MUSE and Marquette are trademarks owned by GE Medical Systems *Information Technologies*, Inc., a General Electric Company going to market as GE Healthcare. All other trademarks contained herein are the property of their respective owners.

The document part number and revision are on each page of the document. The revision identifies the document's update level. The revision history of this document is summarized in the following table.

Revision	Date	Comment
A	20 March 2011	Initial Release of this manual.
B	14 April 2011	Updates to resolve SPR 66469.
C	22 April 2012	Updated the HL7 System State Backup and Recovery chapter with instructions for the G7 server. Updates per SPR 133402 to the HL7 System State Backup and Recovery chapter in sections: Before You Begin (first paragraph 3rd sentence change), RAID Configuration (changes to steps 6 and 14), and Applying the Server Image (changed step 10).
D	5 March 2013	Updated for the HP rp5800 platform. Updated contra indications per SFDA request.

To access other GE Healthcare Diagnostic Cardiology manuals, go to the Common Documentation Library (CDL), located at [www.gehealthcare.com/documents](http://www.gehealthcare.com/documents), and click **Cardiology**.

To access Original Equipment Manufacturer (OEM) manuals, go to the device manufacturer's Web site.

## Service Manual Language Information

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>
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 пациент в резултат на токов удар или 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>• 如果维修服务提供商需要非英文版本，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人员，操作员或患者造成触电、机械伤害或其他形式的伤害。</li></ul>

## Service Manual Language Information (cont'd.)

警告 (ZH-TW)	<p>本維修手冊只提供英文版。</p> <ul style="list-style-type: none"> <li>如果客戶的維修人員有英語以外的其他語言版本需求，則由該客戶負責 提供翻譯服務。</li> <li>除非您已詳閱本維修手冊並了解其內容，否則切勿嘗試對本設備進行維修。</li> <li>不重視本警告可能導致維修人員、操作人員或病患因電擊、機械因素或 其他因素而受到傷害。</li> </ul>
UPOZORENJE (HR)	<p>Ove upute za servisiranje dostupne su samo na engleskom jeziku.</p> <ul style="list-style-type: none"> <li>Ukoliko korisnički servis zahtijeva neki drugi jezik, korisnikova je odgovornost osigurati odgovarajući prijevod.</li> <li>Nemojte pokušavati servisirati opremu ukoliko niste konzultirali i razumjeli ove upute.</li> <li>Nepoštivanje ovog upozorenja može rezultirati ozljedama servisnog osoblja, korisnika ili pacijenta prouzročenim električnim udarom te mehaničkim ili nekim drugim opasnostima.</li> </ul>
VAROVÁNÍ (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 varování 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 medmindre denne servicemanual har været konsulteret og er forstået.</li> <li>Manglende overholdelse af denne advarsel kan medføre skade på grund af elektrisk, mekanisk eller anden fare for teknikeren, operatøren eller patienten.</li> </ul>
WAARSCHUWING (NL)	<p>Deze service manual is alleen in het Engels verkrijgbaar.</p> <ul style="list-style-type: none"> <li>Indien het onderhoudspersoneel een andere taal nodig heeft, dan is de klant verantwoordelijk voor de vertaling ervan.</li> <li>Probeer de apparatuur niet te onderhouden voordat deze service manual geraadpleegd en begrepen is.</li> <li>Indien deze waarschuwing niet wordt opgevolgd, zou het onderhoudspersoneel, de gebruiker of een patiënt gewond kunnen raken als gevolg van een elektrische schok, mechanische of andere gevaren.</li> </ul>
HOIATUS (ET)	<p>Käesolev teenindusjuhend on saadaval ainult inglise keeles.</p> <ul style="list-style-type: none"> <li>Kui klienditeeninduse osutaja nõuab juhendit inglise keelest 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 eiramine võib põhjustada teenuseosutaja, operaatori või patsiendi vigastamist elektrilöögi, mehaanilise või muu ohu tagajärjel.</li> </ul>

## Service Manual Language Information (cont'd.)

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 käännöksen hankkiminen on asiakkaan vastuulla.</li> <li>Älä yritä korjata laitteistoa ennen kuin olet varmasti lukenut ja ymmärtänyt tämän huolto-ohjeen.</li> <li>Mikäli tätä varoitusta ei noudateta, seurauksena voi olla huoltohenkilöstön, laitteiston käyttäjän tai potilaan vahingoittuminen sähköiskun, mekaanisen vian tai muun vaaratilanteen vuoksi.</li> </ul>
ATTENTION (FR)	<p>Ce manuel technique n'est disponible qu'en anglais.</p> <ul style="list-style-type: none"> <li>Si un service technique client souhaite obtenir ce manuel dans une autre langue que l'anglais, il devra prendre en charge la traduction et la responsabilité du contenu.</li> <li>Ne pas tenter d'intervenir sur les équipements tant que le manuel technique 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 ist nur in englischer Sprache verfügbar.</p> <ul style="list-style-type: none"> <li>Falls der Kundendienst eine andere Sprache benötigt, muss er für eine entsprechende Übersetzung sorgen.</li> <li>Keine Wartung durchführen, ohne diese Serviceanleitung gelesen und verstanden zu haben.</li> <li>Bei Zuwiderhandlung kann es zu Verletzungen des Kundendiensttechnikers, des Anwenders oder des Patienten durch Stromschläge, mechanische oder sonstige Gefahren kommen.</li> </ul>
ΠΡΟΕΙΔΟΠΟΙΗΣΗ (GR)	<p>Το παρόν 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>Μην επιχειρήσετε 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>
FIGYELMEZTETÉS (HU)	<p>Ez a szerviz kézikönyv kizárólag angol nyelven érhető el.</p> <ul style="list-style-type: none"> <li>Ha a vevő szerviz ellátója angoltól eltérő nyelvre tart igényt, akkor a vevő felelőssége a fordítás elkészítése.</li> <li>Ne próbálja elkezdni használni a berendezést, amíg a szerviz kézikönyvben leírtakat nem értelmezték és értették meg.</li> <li>Ezen figyelmeztetés figyelmen kívül hagyása a szerviz ellátó, a működtető vagy a páciens áramütés, mechanikai vagy egyéb veszélyhelyzet miatti sérülését eredményezheti.</li> </ul>
ADVÖRUN (IS)	<p>Þessi þjónustuhandbók er eingöngu fánleg á ensku.</p> <ul style="list-style-type: none"> <li>Ef að þjónustuveitandi viðskiptamanns þarfnast annars tungumáls en ensku, er það skylda viðskiptamanns að skaffa tungumálþjónustu.</li> <li>Reynið ekki að afgreiða tækið nema þessi þjónustuhandbók hefur verið skoðuð og skilin.</li> <li>Brot á að sinna þessari aðvörun getur leitt til meiðsla á þjónustuveitanda, stjórnaða eða sjúklingi frá raflösti, vélrænum eða öðrum áhættum.</li> </ul>

## Service Manual Language Information (cont'd.)

PERINGATAN (ID)	<p>Manual servis ini hanya tersedia dalam bahasa Inggris.</p> <ul style="list-style-type: none"> <li>Jika penyedia jasa servis pelanggan memerlukan bahasa lain selain dari Bahasa Inggris, merupakan tanggung jawab dari penyedia jasa servis tersebut untuk menyediakan terjemahannya.</li> <li>Jangan mencoba melakukan servis terhadap perlengkapan kecuali telah membaca dan memahami manual servis ini.</li> <li>Mengabaikan peringatan ini bisa mengakibatkan cedera pada penyedia servis, operator, atau pasien, karena terkena kejut listrik, bahaya mekanis atau bahaya lainnya.</li> </ul>
AVVERTENZA (IT)	<p>Il presente manuale di manutenzione è disponibile soltanto in Inglese.</p> <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>Si proceda alla manutenzione dell'apparecchiatura solo dopo aver consultato il presente manuale ed averne compreso il contenuto.</li> <li>Il non rispetto della presente avvertenza potrebbe far compiere operazioni da cui derivino lesioni all'addetto, alla manutenzione, all'utilizzatore ed al paziente per folgorazione elettrica, per urti meccanici od altri rischi.</li> </ul>
警告 (JA)	<p>このサービスマニュアルは英語版しかありません。</p> <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、十分に理解をした上で装置のサービスを行ってください。</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)	<p>본 서비스 지침서는 영어로만 이용하실 수 있습니다.</p> <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 지침서를 참고했고 이해하지 않는 한은 해당 장비를 수리하려고 시도하지 마십시오.</li> <li>이 경고에 유의하지 않으면 전기 쇼크, 기계상의 혹은 다른 위험으로부터 서비스 제공자, 운전자 혹은 환자에게 위험을 가할 수 있습니다.</li> </ul>
BRĪDINĀJUMS (LV)	<p>Šī apkopotāju rokasgrāmata ir pieejama tikai angļu valodā.</p> <ul style="list-style-type: none"> <li>Ja apkalošanas sniedzējam nepieciešama informācija citā, nevis angļu, valodā, klienta pienākums ir nodrošināt tās tulkošanu.</li> <li>Neveiciet aprīkojuma apkopi, neizlasot un nesaprotot apkopotāju rokasgrāmatu.</li> <li>Šī brīdinājuma neievērošana var radīt elektriskās strāvas trieciena, mehānisku vai citu risku izraisītu traumu apkopes sniedzējam, operatoram vai pacientam.</li> </ul>
ĮSPĖJIMAS (LT)	<p>Šis eksploatavimo vadovas yra prieinamas tik anglų kalba.</p> <ul style="list-style-type: none"> <li>Jei kliento paslaugų tiekėjas reikalauja vadovo kita kalba - ne anglų, numatyti vertimo paslaugas yra kliento atsakomybė.</li> <li>Nemėginkite atlikti įrangos techninės priežiūros, nebent atsižvelgėte į šį eksploatavimo vadovą ir jį supratote.</li> <li>Jei neatkreipsite dėmesio į šį perspėjimą, galimi sužalojimai dėl elektros šoko, mechaninių ar kitų paslaugų tiekėjui, operatoriui ar pacientui.</li> </ul>

## Service Manual Language Information (cont'd.)

ADVARSEL (NO)	<p>Denne servicehåndboken finnes bare på engelsk.</p> <ul style="list-style-type: none"> <li>• Hvis kundens serviceleverandør trenger 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>
OSTRZEŻENIE (PL)	<p>Niniejszy podręcznik serwisowy dostępny jest jedynie w języku angielskim.</p> <ul style="list-style-type: none"> <li>• Jeśli dostawca usług klienta wymaga języka innego niż angielski, zapewnienie usługi tłumaczenia jest obowiązkiem klienta.</li> <li>• Nie należy serwisować wyposażenia bez zapoznania się i zrozumienia niniejszego podręcznika serwisowego.</li> <li>• Niezastosowanie się do tego ostrzeżenia może spowodować urazy dostawcy usług, operatora lub pacjenta w wyniku porażenia elektrycznego, zagrożenia mechanicznego bądź innego.</li> </ul>
AVISO (PT-BR)	<p>Este manual de assistência técnica só se encontra disponível em inglês.</p> <ul style="list-style-type: none"> <li>• Se o serviço de assistência técnica do cliente não for GE, e precisar de outro idioma, será 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 por em perigo a segurança do técnico, operador ou paciente devido a choques elétricos, mecânicos ou outros.</li> </ul>
AVISO (PT-PT)	<p>Este manual técnico só se encontra disponível em inglês.</p> <ul style="list-style-type: none"> <li>• Se a assistência técnica do cliente solicitar estes manuais 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 técnico.</li> <li>• O não cumprimento deste aviso pode provocar lesões ao técnico, ao utilizador ou ao paciente devido a choques eléctricos, mecânicos ou outros.</li> </ul>
AVERTISMENT (RO)	<p>Acest manual de service este disponibil numai 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 înțelegerii 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>
ПРЕДУПРЕЖДЕНИЕ (RU)	<p>Настоящее руководство по обслуживанию предлагается 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 обеспечить перевод самостоятельно.</li> <li>• Прежде чем приступать к обслуживанию оборудования, обязательно обратитесь к настоящему руководству и внимательно изучите изложенные в нем сведения.</li> <li>• Несоблюдение требований данного предупреждения может привести к тому, что специалисты по обслуживанию, операторы или пациенты получат удар электрическим током, механическую травму или другое повреждение.</li> </ul>

## Service Manual Language Information (cont'd.)

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 povređivanja serviser, rukovaoca ili pacijenta usled strujnog udara, ili mehaničkih i drugih opasnosti.</li> </ul>
VAROVANIE (SK)	<p>Tento návod na obsluhu je k dispozícii len v angličtine.</p> <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 skôr, ako si neprečítate návod na obsluhu a neporozumiete mu.</li> <li>Zanedbanie tohto varovania môže vyústiť do zranenia poskytovateľa služieb, obsluhujúcej osoby alebo pacienta elektrickým prúdom, mechanickým alebo iným nebezpečenstvom.</li> </ul>
OPOZORILO (SL)	<p>Ta servisni priročnik je na voljo samo v angleškem jeziku.</p> <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>
ADVERTENCIA (ES)	<p>Este manual de servicio sólo existe en inglés.</p> <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)	<p>Den här servicehandboken finns bara tillgänglig på engelska.</p> <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 förstår 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>
UYARI (TR)	<p>Bu servis kılavuzunun sadece İngilizcesi mevcuttur.</p> <ul style="list-style-type: none"> <li>Eğer müşteri teknisyeni bu kılavuzu İngilizce dışında bir başka lisandan talep ederse, bunu tercüme ettirmek müşteriye düşer.</li> <li>Servis kılavuzunu okuyup anlamadan ekipmanlara müdahale etmeyiniz.</li> <li>Bu uyarıya uyulmaması, elektrik, mekanik veya diğer tehlikelerden dolayı teknisyen, operatör veya hastanın yaralanmasına yol açabilir.</li> </ul>

## Service Manual Language Information (cont'd.)

<p>ЗАСТЕРЕЖЕННЯ (UK)</p>	<p>Дане керівництво з сервісного обслуговування постачається виключно англійською мовою.</p> <ul style="list-style-type: none"> <li>• Якщо сервісний інженер потребує керівництво іншою мовою, користувач зобов'язаний забезпечити послуги перекладача.</li> <li>• Не намагайтеся здійснювати технічне обслуговування даного обладнання, якщо ви не читали, або не зрозуміли інформацію, надану в керівництві з сервісного обслуговування.</li> <li>• Недотримання цього застереження може призвести до травмування сервісного інженера, користувача даного обладнання або пацієнта внаслідок електричного шоку, механічного ушкодження або з інших причин невірної обслуговування обладнання.</li> </ul>
<p>CẢNH BÁO (VI)</p>	<p>Tài Liệu Hướng Dẫn Sửa Chữa chỉ có bản tiếng Anh.</p> <ul style="list-style-type: none"> <li>• Nếu các đơn vị cung cấp dịch vụ cho khách hàng yêu cầu một ngôn ngữ nào khác tiếng Anh, thì khách hàng sẽ có trách nhiệm cung cấp các dịch vụ dịch thuật.</li> <li>• Không được sửa chữa thiết bị trừ khi đã tham khảo và hiểu Tài liệu Hướng dẫn Sửa chữa.</li> <li>• Không tuân thủ những cảnh báo này có thể dẫn đến các tổn thương cho người thực hiện sửa chữa, người vận hành hay bệnh nhân, do sốc điện, các rủi ro về cơ khí hay các rủi ro khác.</li> </ul>



# Contents

## 1 Introduction

Indications for Use .....	15
Contraindications .....	15
System Accuracy.....	15
Prescription Device Statement .....	15
<b>Regulatory and Safety Information.....</b>	<b>16</b>
Safety Conventions .....	16
Safety Hazards.....	16
RF Caution .....	19
EMI/EMC Requirements .....	19
Equipment Compliance .....	20
Parts and Accessories Information.....	21
Responsibility of the Manufacturer.....	22
Responsibility of the Purchaser/Customer.....	22
Symbols .....	22
<b>Training.....</b>	<b>25</b>
<b>Service Information.....</b>	<b>25</b>
Service Requirements .....	25
Customer-supplied Hardware.....	26
Hardware Supplied by GE Healthcare .....	26
Security Updates .....	26
Additional Assistance .....	26
<b>Manual Information .....</b>	<b>26</b>
Intended Audience .....	27
Manual Purpose .....	27
Document Conventions .....	27
<b>Related Documents.....</b>	<b>28</b>

## 2 Product Overview

General Operation .....	29
Data Acquisition.....	30
<b>Device Interfaces .....</b>	<b>31</b>
MAC Carts.....	31
MARS .....	32
CASE/CardioSoft Stress Systems .....	32
Monitoring Systems.....	32
Modems.....	32

HL7 Interface .....	33
Optional Features .....	34
Hardware Specifications .....	37
Software Specifications.....	37
<b>The MUSE System in Virtual Environments .....</b>	<b>37</b>
Customer Responsibilities.....	38
Data Acquisition .....	38
HL7 Interface Virtual Machine .....	38
<b>MUSE v8 Drive Contents and Supporting Folders .....</b>	<b>38</b>
Muse Application and Database on Same Server .....	39
MUSE Application and Database on Separate Servers.....	39
<b>MUSE Services .....</b>	<b>40</b>
<b>Required Network Ports .....</b>	<b>41</b>

### 3 System Setup

<b>Setting Up Modems .....</b>	<b>43</b>
Verifying/Installing the MUSE Modem Service and Wireless/LAN Communication.....	43
Setting Up a Modem Device.....	44
Restarting Modems .....	45
Testing CSI Network Modem Connections .....	47
<b>Installing and Configuring the XML Import Option .....</b>	<b>48</b>
Installing the XML Import Option and MUSE XML Service.....	48
Requirements .....	48
Using XMLCONFIG.EXE to Configure the Option on MUSE.....	48
<b>Setting Up the MUSE File Server for File Copy .....</b>	<b>50</b>
Setting Up a Folder.....	51
<b>MUSE Authentication—Enable or Disable .....</b>	<b>51</b>
<b>Configuring Windows High Contrast Color Scheme on MUSE Client.....</b>	<b>52</b>
<b>Changing MUSE Service Accounts.....</b>	<b>53</b>
MUSE User Service Accounts.....	53
MUSE Windows User Service Accounts .....	53
Changing the MUSE User Account Passwords.....	53

### 4 System Administration

<b>Remote Databases.....</b>	<b>55</b>
SQL Ports .....	55
SQL Remote Connections .....	56
<b>AutoShutdown .....</b>	<b>56</b>
Activating System Shutdown.....	56
Canceling the System Shutdown .....	58

<b>Modifying the MUSE Installed Configuration .....</b>	<b>58</b>
<b>Moving the MUSE Databases .....</b>	<b>59</b>
Preparing the New Database Server.....	60
Detaching and Copying the MSUE Databases from the Current Server.....	60
Attaching the MUSE Databases to the New SQL Server.....	60
<b>Uninstalling/Reinstalling the MUSE Application .....</b>	<b>61</b>
Uninstalling the MUSE Application .....	61
Reinstalling the MUSE Application.....	61
<b>Renaming the MUSE Server.....</b>	<b>62</b>
<b>Changing the Port Number of the File Server .....</b>	<b>63</b>
Changing the Port Number on the MUSE Server .....	63
Changing the Port Number on the MUSE Clients .....	64
<b>BIOS Updates .....</b>	<b>64</b>
Upgrading the G4 Server BIOS Firmware .....	64

## **5 Maintenance**

<b>Maintenance Guidelines.....</b>	<b>67</b>
OEM Maintenance.....	68
Required Tools and Supplies.....	68
<b>Inspection and Cleaning .....</b>	<b>68</b>
Safe Shutdown Procedures.....	69
Precautions.....	69
Visual Inspection.....	70
Check Cooling Fans and Ventilation .....	70
Exterior Cleaning .....	71
<b>Functional Checkout Procedures .....</b>	<b>71</b>
Hardware FRU Repairs .....	71
Non-FRU Repairs .....	76

## **6 HL7 System State Backup and Recovery**

<b>Copying the System State Backup .....</b>	<b>83</b>
<b>Disaster Recovery .....</b>	<b>83</b>
Before You Begin .....	83
<b>Rebuilding the HP DL360 G5 Server .....</b>	<b>84</b>
Configuring the Server.....	84
Configuring the RAID.....	85
Installing Windows Server 2003 .....	86
Configuring Display Settings .....	87
Setting Up the Windows Environment.....	87
Installing Windows 2003 Service pack 2.....	87
<b>Rebuilding the HP DL360 G7 Server .....</b>	<b>87</b>
Verify the Boot Sequence .....	88
RAID Configuration.....	88
Applying the Server Image.....	89
<b>Verify Help and Support Service .....</b>	<b>90</b>

	Configuring SNMP .....	90
	Installing CCG.....	91
	Installing InSite ExC.....	91
	Restoring System State.....	91
<b>7</b>	<b>MUSE System Backup and Recovery</b>	
	Introduction .....	93
	Backup Options .....	94
	Overview of the MUSE Disk and Data Structures .....	94
	Overview of the Network and Tape Backup Options.....	95
	Setting Up Automatic Backups .....	97
	Creating Backup Jobs .....	98
	Configuring the Backup Jobs.....	99
	Changing the Backup Schedule .....	102
	Creating Notifications .....	103
	Testing the Backup Jobs .....	107
	Backing Up the Database Manually .....	109
	Database Recovery .....	109
	Copying the Current Database.....	110
	Recovering the MUSE Database.....	110
	Reverting to the Current Database.....	115
	Additional Information.....	115
	System Shutdown and Restart Procedure.....	115
	Initializing a New Tape.....	116
<b>A</b>	<b>System Recovery</b>	
	Using Recovery Console .....	117
	Server Recovery Using a Network Backup .....	118
	Reimaging the HP ML370 G5 Server .....	118
	Reimaging the HP DL370 G6 Server .....	119
	Recovering the System Partition (C: Drive).....	122
	Adding the Server to the Domain.....	123
	Recovering the Data Partition (D: Drive).....	124
	Restoring the MUSE Databases.....	125
	Verifying the MUSE Communications.....	125
	Restoring Other Functionality .....	125
	Server Recovery Using a Tape Backup .....	125
	Using Automated System Recovery.....	126
	Configuring the File Server RAID Array .....	126
	Recovering the System Partition.....	128
	Recovering the MUSE Databases.....	129
	Other Tasks to Perform After System Restore.....	130
	Client Rebuild .....	130
	Setting SATA Emulation and Boot Order (All Configurations).....	131
	Loading the Image .....	132

Configuring the Operating System .....	133
Activating the Operating System .....	136
Reinstalling the MUSE Application.....	137

## **B Electromagnetic Compatibility**

<b>Electromagnetic Compatibility for DL370 G6 Server.....</b>	<b>139</b>
Electromagnetic Compatibility (EMC) Requirements .....	139
Guidance and Manufacturer's Declaration—Electromagnetic Emissions.....	141
Guidance and Manufacturer's Declaration—Electromagnetic Immunity .....	141
Guidance and Manufacturer's Declaration—Electromagnetic Immunity .....	143
Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL370 G6 Server.....	144
EMC Exception(s) Disclosure.....	145
<b>Electromagnetic Compatibility for ML370 G5 Server .....</b>	<b>146</b>
Electromagnetic Compatibility Requirements (EMC) .....	146
Guidance and Manufacturer's Declaration—Electromagnetic Emissions.....	147
Guidance and Manufacturer's Declaration—Electromagnetic Immunity .....	148
Guidance and Manufacturer's Declaration—Electromagnetic Immunity .....	150
Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL360 G5 Server.....	152
EMC Exception(s) Disclosure .....	152

## **C National Health Service of Great Britain (NHS) Patient Identifiers**

<b>Purpose .....</b>	<b>155</b>
<b>Overview .....</b>	<b>155</b>
<b>Number Validation .....</b>	<b>155</b>
<b>Number Verification .....</b>	<b>156</b>
<b>Searching by Patient ID (PID).....</b>	<b>157</b>
<b>Displaying the Patient ID .....</b>	<b>157</b>
<b>Updating Legacy System Data .....</b>	<b>158</b>
<b>Installing the NHS Number Feature .....</b>	<b>159</b>
<b>Modules and Files Affected .....</b>	<b>159</b>

## **D Glossary**

.....	163
-------	-----



# Introduction

This chapter provides general information required for the proper use of the system and this manual. Familiarize yourself with this information before using the system.

## Indications for Use

The MUSE Cardiology Information System is intended to store, access and manage cardiovascular information on adult and pediatric patients. The information consists of measurements, text, and digitized waveforms. The MUSE Cardiology Information System provides the ability to review and edit electrocardiographic procedures on screen, through the use of reviewing, measuring, and editing tools including ECG serial comparison. The MUSE Cardiology Information System is intended to be used under the direct supervision of a licensed healthcare practitioner, by trained operators in a hospital or facility providing patient care.

## Contraindications

**WARNING:**

CONTRAINDICATION: The system is not intended for pediatric serial comparison.

**WARNING:**

CONTRAINDICATION: The system is not intended for real-time patient monitoring.

## System Accuracy

Accuracy of the MUSE system is 100% data reproduction, dependent on zoom settings, and resolution of display and/or printer being used.

## Prescription Device Statement

**CAUTION:**

United States federal law restricts this device to sale by or on the order of a physician.

# Regulatory and Safety Information

This section provides information about the safe use and regulatory compliance of this system. Familiarize yourself with this information, and read and understand all instructions before attempting to use this system. The system software is considered medical software. As such, it was designed and manufactured to the appropriate medical regulations and controls.

**NOTE:**

Disregarding the safety information provided in this manual is considered abnormal use of this system and could result in injury, data loss, or a voided warranty.

## Safety Conventions

A **Hazard** is a source of potential injury to a person, property, or the system.

This manual uses the terms DANGER, WARNING, CAUTION, and NOTICE to point out hazards and to designate a degree or level of seriousness. Familiarize yourself with the following definitions and their significance.

### Definitions of Safety Conventions

Safety Convention	Definition
<b>DANGER</b>	Indicates an imminent hazard, which, if not avoided, will result in death or serious injury.
<b>WARNING</b>	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in death or serious injury.
<b>CAUTION</b>	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in moderate or minor injury.
<b>NOTICE</b>	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in the loss or destruction of property or data.

## Safety Hazards

The following messages apply to the system as a whole. Specific messages may also be provided elsewhere in the manual.

**DANGER:**

EXPLOSION HAZARD: Flammable anesthetic vapors or liquids can cause explosions.

Do NOT use in the presence of flammable anesthetic vapors or liquids.

**WARNING:**

ACCIDENTAL SPILLS: If liquids have entered the system, take it out of service and have it checked by a service technician before it is used again.

To avoid electric shock or device malfunction, liquids must not be allowed to enter the system.



**WARNING:**

CONNECTION TO MAINS: This is Class I equipment.

The mains plug must be connected to an appropriate power supply.

The file server may contain an internal battery pack. There is risk of fire and burns if the battery pack is not handled properly. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose to temperatures higher than 60° C (140° F).
- Do not disassemble, crush, puncture, short external contacts or dispose of in fire or water.
- Replace only with the appropriate spare parts designated for this product.

**WARNING:**

DATA LOSS OR CORRUPTION: DO NOT load any software other than that specified by GE Healthcare onto the MUSE system. Installation of software not specified by GE Healthcare may cause damage to the equipment, or loss or corruption of data.

**WARNING:**

DELAY IN TREATMENT: This device is not intended for real-time monitoring.

**WARNING:**

ELECTRIC SHOCK: To reduce the risk of electric shock, do NOT remove cover (or back).

Refer servicing to qualified personnel.

**WARNING:**

ELECTRIC SHOCK: Improper use of this device presents a shock hazard. Strictly observe the following warnings. Failure to do so may endanger the lives of the user, and bystanders.

When disconnecting the device from the power line, remove the plug from the wall outlet first, before disconnecting the cable from the device; otherwise, there is a risk of coming in contact with line voltage by inadvertently introducing metal parts in the sockets of the power cord.

Devices may be connected to other devices or to parts of systems only after making certain that there is no danger to the patient, the operators, or the environment as a result. Standards EN/IEC 60601-1-1 must be complied with in all cases.

**WARNING:**

EMI PERFORMANCE HAZARD: Users should be aware of known Radio Frequency (RF) sources, such as:

- radio and TV stations
- portable and mobile RF communication devices (cell phones, two-way radios)

and consider them when installing the medical device or system.

See the "Electromagnetic compatibility" section found either in this manual and/or the service manual for recommended separation distances.

Adding accessories or components, or modifying the medical device or system may degrade the Electromagnetic Interference (EMI) performance. Consult with qualified personnel regarding changes to the system configuration.

**WARNING:**

EXPLOSION HAZARD: Flammable anesthetic vapors or liquids can cause explosions.

Do NOT use in the presence of flammable anesthetic vapors or liquids.

**WARNING:**

INCORRECT TREATMENT: Failure to have a unique Patient ID (PID) in patient demographics may cause incorrect patient data associated with the PID.

Always assign the proper PID and name before transmission to the MUSE system. Do not confirm patient records containing default PIDs. For more information concerning PIDs, see the ***MUSE Cardiology Information System Operator's Manual***.

**WARNING:**

INCORRECT TREATMENT: Some of the communications protocols used in this product (CSI and DCP) do not provide encryption or authentication at this time. These protocols are used to send clinical data to the system from ECG carts and other clinical devices.

You should take appropriate steps to secure the privacy of communications on your network when using this product.

**WARNING:**

LOSS OF DATA: Database backup is the responsibility of the customer.

GE Medical Systems *Information Technologies*, Inc. is not responsible for data loss of any kind as a result of customer's failure to backup data.

**WARNING:**

PATIENT SAFETY: All computer-generated tracings should be overread by a qualified physician.

**WARNING:**

DATA LOSS OR CORRUPTION: Installation of software not specified by GE Healthcare may cause damage to the equipment, loss or corruption of data.

DO NOT load any software other than that specified by GE Healthcare onto the system.

**WARNING:**

LOSS OF DATA: Changing settings without knowing how they affect the system can cause loss of data.

Do not change any current settings unless you understand how the change affects the system.

**WARNING:**

PERSONAL INJURY Falling objects may cause severe injury.

Be sure that the server is adequately stabilized.

**CAUTION:**

DATA LOSS OR SYSTEM FAILURE: Data loss or system failure can result due to ingress of liquids. The system does not provide protection against ingress of liquids.

Ensure installation in a cool, dry environment.

**CAUTION:**

EQUIPMENT INTERFERENCE Equipment or system should not be used adjacent to, or stacked with, other equipment.

If adjacent or stacked use is necessary, the equipment or system should be tested to verify normal operation in that configuration.

**NOTE:**

MUSE system operation may be affected if large machines with high current draws are connected to the same electrical circuit as the MUSE system. It is recommended that the MUSE system be connected to a power source away from these machines.

**NOTE:**

If a UPS was provided by GE Healthcare, do not connect your laser printer to the UPS. In some environments, the cycling of power in the laser printer can trigger the low voltage alarm on the UPS.

## RF Caution

Radio Frequency (RF) devices may interfere with the use or accuracy of the device or system. When installing or using the device or system, you should consider the proximity of known RF sources, such as:

- Radio and TV stations
- Portable and mobile RF communication devices (cell phones, two-way radios)
- X-ray, CT, or MRI devices  
These devices are also a possible source of interference as they may emit higher levels of electromagnetic radiation.

**WARNING:**

EQUIPMENT: Do not use the device or system adjacent to or stacked with other equipment. If adjacent or stacked use is necessary, observe the device or system to verify normal operation in the configuration in which it is being used.

See the *Electromagnetic Compatibility* section found in the service manual for recommended separation distances.

**WARNING:**

ACCESSORIES/COMPONENTS: Adding accessories or components, or modifying the medical device or system, may result in increased EMISSIONS or decreased IMMUNITY of the device or system.

- See the supplies and accessories manual for your system for qualified accessories and/or components, if applicable.
- Consult with qualified personnel regarding changes to the device or system configuration.

## EMI/EMC Requirements

This device or system is labeled under the original equipment manufacturers label (for example, USA FCC 47CFR15, CE EU EMC 2004/108/EC), and deemed sufficient by GE Healthcare to be in compliance with EN/IEC 60601-1-2 when used according to the device or system's intended use. Hardware supplied by GE Healthcare meets the applicable country requirements.

Changes or modifications to this system not expressly approved by GE Healthcare could cause EMC issues with this or other equipment. This system is designed and tested to comply with applicable regulations regarding EMC, and must be installed and put into service according to the EMC information stated in the EMC chapter located in the service manual for this system.

**WARNING:**

EQUIPMENT MALFUNCTION – The use of portable phones or other radio frequency (RF) emitting equipment near the system may cause unexpected or adverse operation.

Do not use portable phones or other electronic equipment that may emit radio frequency (RF) near this system.

**WARNING:**

EQUIPMENT MALFUNCTION – Do not use the equipment or system adjacent to, or stacked with, other equipment.

If adjacent or stacked use is necessary, test the equipment or system to verify normal operation in the configuration in which you are using it.

Classification	Description
Class A	The device or system is suitable for use in all establishments, other than domestic and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes. Mains power should be a typical commercial or hospital environment.
Class B	The device or system is suitable for use in all establishments, including domestic establishments and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes.

**NOTE:**

Compliance provides reasonable protection against radio-frequency interference. However, there is no guarantee that interference will not occur in a particular installation. You can tell whether this device or system is causing interference by turning it off. If the interference stops, it was probably caused by the device or system.

## Equipment Compliance

The device or system is labeled under the original equipment manufacturer's label (for example, UL, CE EU LVD 2006/95/EC) and deemed sufficient by GE Healthcare to be in compliance with EN/IEC 60601-1 (clause 3.201.2 for use of non-medical devices in a medical system), when used according to the device or system's intended use. Hardware supplied by GE Healthcare meets the applicable country requirements for Information Technology Equipment (ITE).

## Information Technology Equipment Requirements

The hardware components of the system are not considered medical equipment. They are considered Information Technology Equipment (ITE). The system's individual components comply with the standards for Safety of Information Technology Equipment (for example, UL 60950-1, EN/IEC 60950-1).

If you use the system in a patient's vicinity, it must comply with the standard requirements for medical systems (that is, EN/IEC 60601-1).

- To comply with this standard, you must connect the components and all attached accessories to a medical grade (EN/IEC 60601-1) power source (for example, Medical grade UPS or Isolation Transformer).
- System Inputs/Outputs connected to non-medical equipment must also be isolated for overall system compliance.
- Patient vicinity is defined as a space, within a location intended for the examination and treatment of patients, extending 1.83m (6 ft.) beyond the normal location of the bed, chair, table, treadmill, or other device(s) supporting the patient during examination and treatment, and extending vertically to 2.5m (8 ft. 2.4 in.) above the floor.

In addition, any non-medical electrical equipment that you use with the system (outside the patient vicinity) must comply with applicable safety standards for that equipment (that is, EN/IEC 60950-1).

**NOTE:**

If the equipment is installed in the U.S.A. using 240V rather than 120V, the source must be a center-tapped, 240V, single-phase circuit.

## Parts and Accessories Information

**WARNING:**

**PATIENT SAFETY** — To ensure patient safety, use only parts and accessories manufactured or recommended by GE Healthcare.

Contact GE Healthcare for information before connecting any devices to this equipment that are not recommended in this manual.

If the installation of this equipment in the U.S.A. uses 240V rather than 120V, the source must be a center-tapped, 240V, single-phase circuit.

Parts and accessories must meet the requirements of the applicable 60601 safety standards, and/or the system configuration must meet the requirements of the 60601-1-1 Medical Electrical Systems standard.

Using accessory equipment that does not comply with the equivalent safety requirements of this equipment may lead to a reduced level of safety of the resulting system. Consideration relating to the choice shall include:

- Use of the accessory in the Patient Vicinity.  
Patient vicinity is defined as a space, within a location intended for the examination and treatment of patients, extending 1.83m (6 ft.) beyond the normal location of the bed, chair, table, treadmill, or other device(s) supporting the patient during examination and treatment, and extending vertically to 2.5m (8 ft. 2.4 in.) above the floor.
- Evidence that the safety certification of the accessory was performed in accordance with the appropriate 60601-1 and/or 60601-1-1 standard(s).

## Responsibility of the Manufacturer

GE Healthcare is responsible for the safety, reliability, and performance of hardware supplied by GE Healthcare only if the following conditions are met:

- Assembly operations, extensions, readjustments, modifications, or repairs are performed by persons authorized by GE Healthcare.
- The electrical installation of the room where the device is used complies with the requirements of the appropriate local, state, and other government regulations.
- The equipment is used in accordance with the instructions for use.

## Responsibility of the Purchaser/Customer

The customer is responsible for providing appropriate desks, chairs, electrical wall outlets, network connections, and analog phone lines, and for locating any of the system components described in this manual in compliance with all local, state, and national codes.

## Symbols

The following symbols may appear on the device or its packaging. Familiarity with these symbols assists in the safe use and disposal of the equipment. For equipment symbols not shown, refer to the original equipment manufacturers (OEM) manuals.




The OEM devices included with the system are as follows (see the *MUSE Cardiology Information System Service Manual* for a complete list and names of OEM devices):

- Monitor(s)
- File Server
- Client
- Modem(s)










### NOTE:

All symbols indicated/defined in this manual may or may not appear on the product.















### Equipment Symbols

Symbol	Description
	<b>CAUTION:</b> Consult accompanying documents.
	Indicates the presence of hazardous energy circuits or electric shock hazards. <b>WARNING:</b> ELECTRIC SHOCK To reduce the risk of electric shock, do NOT remove front or back cover. Refer servicing to qualified personnel.
	<b>CAUTION:</b> SAFETY GROUND PRECAUTION Remove power cord from the mains source by grasping the plug. DO NOT pull on the cable.

## Equipment Symbols (cont'd.)



	Indicates that the waste of electrical and electronic equipment must not be disposed as unsorted municipal waste and must be collected separately. Please contact an authorized representative of the manufacturer for information concerning the decommissioning of your equipment.
	Date of Manufacture (Year-Month).
	Indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists. <b>WARNING:</b> HOT SURFACE/COMPONENT To reduce the risk of injury from a hot component, allow the surface to cool before touching.
	This symbol on an RJ-45 receptacle indicates a Network Interface Connection. <b>WARNING:</b> ELECTRIC SHOCK To reduce the risk of electric shock, fire or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.
	Indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason. <b>WARNING:</b> ELECTRIC SHOCK To reduce the risk of electric shock hazards, do not open this enclosure.
	These symbols on power supplies or systems indicate the equipment is supplied by multiple sources of power. <b>WARNING:</b> ELECTRIC SHOCK To reduce the risk of injury from electric shock, remove all power cords to completely disconnect power from the system.
	Indicates the component exceeds the recommended weight for one individual to handle safely. <b>WARNING:</b> INJURY/DAMAGE To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.
	Humidity limitations.
	Atmospheric pressure limitation.

## Equipment Symbols (cont'd.)

 <b>ABC123</b>	Batch code of paper or battery.
	Manufacturer name and address.
	CE Mark - Symbolizes conformity with applicable EU (European Union) directives
	PCT (GOST-R) Mark - Symbolizes compliance with applicable requirements for Russia
 <b>ABC123</b>	Serial number.
 <b>ABC123</b>	Catalog number.
 <b>Company Address</b>	European authorized representative.
	The packaging of this product can be recycled.
	Indicates the product is classified as CLASS 1 LASER PRODUCT. Located on the surface of your laser device.
	CD headphone jack.
	Adjustment control dial.
	CD eject button.
 <b>READ DISKETTE</b>	Scanning the bar code with the bar code reader allows you to acquire records from a diskette.
	Indicates the presence of a sharp edge or object that can cause cuts or other bodily injury. <b>WARNING:</b> BODILY INJURY To prevent cuts or other bodily injury, do not contact sharp edge or object.



## Equipment Symbols (cont'd.)

	<p>Indicates the presence of mechanical parts that can result in pinching, crushing or other bodily injury.</p> <p><b>WARNING:</b> BODILY INJURY To avoid risk of bodily injury, keep away from moving parts.</p>
	<p>Indicates the presence of a potential tip-over hazard that can result in bodily injury.</p> <p><b>WARNING:</b> BODILY INJURY To avoid risk of bodily injury, follow all instructions for maintaining stability of the equipment during transport, installation and maintenance.</p>

## Training

This manual is intended as a supplement to, not a substitute for, thorough product training. If you have not received training on the use of the system, you should request training assistance from GE Healthcare.

To see available training, go to the GE Healthcare training Web site ([www.gehealthcare.com/training](http://www.gehealthcare.com/training)). Select *Education>Product Education-Technical>Diagnostic Cardiology*.

For more self-paced course offerings, tools, and reference guides you may find useful, please visit the GE Healthcare Education Store at [www.gehealthcare.com/educationstore](http://www.gehealthcare.com/educationstore).

## Service Information

This section provides information pertaining to the maintenance and servicing of the system. Familiarize yourself with this information before requesting service from GE Healthcare or its authorized representatives.

## Service Requirements

Failure on the part of the responsible individual, hospital, or institution using this equipment to implement a satisfactory maintenance schedule may cause undue equipment failure and possible safety hazards.

Regular maintenance, irrespective of usage, is essential to ensure that the components of this system are always functional when required.

## Customer-supplied Hardware

Customers who purchase their own equipment are responsible for any repair or maintenance, and for completing equipment checkout after any repair or maintenance.

## Hardware Supplied by GE Healthcare

For hardware supplied by GE Healthcare, only authorized GE Healthcare service personnel should service the equipment. Any unauthorized attempt to repair equipment under warranty voids that warranty. It is the user's responsibility to report the need for service to GE Healthcare or to one of their authorized agents.

## Security Updates

A list of viruses that pose a significant threat to GE Healthcare customers' system security is posted on the GE Healthcare Product Security web site.

As new vulnerabilities and potential security issues arise, GE Healthcare makes every effort to quickly identify and notify customers of approved fixes. Time is required for GE Healthcare to identify the vulnerability, test the fix, and run a validation test on the system for safety and functionality. Only after this rigorous process does GE Healthcare release the official patch. While we recognize the urgency to correct these problems, we must ensure that the integrity of the system is not compromised.

After security patches are validated for specific GE Healthcare systems, the information is added to the Product Security website. You can download the patch directly from the website of the software manufacturer (Microsoft, and so forth) and apply it to your GE Healthcare system. To check on the latest information regarding validated security patches:

1. Browse to the GE Healthcare Product Security website: <http://prodsecdb.gehealthcare.com>  
The **Single Sign On** (SSO) window opens.
2. Enter your SSO number and password and click **Log In**.  
If you do not have an SSO number, click the **Sign Up** link to obtain one.
3. Use the features on the GE Healthcare **Product Security Database** Web site to identify security patches that you can apply to your system.

## Additional Assistance

GE Healthcare maintains a trained staff of application and technical experts to answer questions and respond to issues and problems that may arise during the installation, maintenance, and use of this system.

Contact your local GE Healthcare representative to request additional assistance.

## Manual Information

This section provides information for the correct use of this manual.

Keep this manual with the equipment at all times and periodically review it. You should request training assistance from GE Healthcare, if needed.

## Intended Audience

This manual is intended to be used by trained GE Healthcare service personnel, GE Healthcare-approved third party service personnel, or local biomedical or IT personnel, responsible for administration and maintenance of the MUSE system and the hardware and network environment on which it is running.

This manual does not provide instruction for clinical use of the system. For clinical use of the MUSE system, refer to the ***MUSE Cardiology Information System Operator's Manual***.

## Manual Purpose

This manual provides technical information to service and technical personnel so they can service and maintain the MUSE system. The MUSE system, as defined in this manual, includes the MUSE Application server, MUSE database, MUSE clients, and HL7 Interface server.

Where necessary, the manual identifies additional sources of relevant information and/or technical assistance.

This manual is intended only for use with MUSE v8.x. For earlier versions of MUSE, use the ***MUSE Cardiology Information System Service Manual*** that originally shipped with your product. See the ***MUSE Cardiology Information System Operator's Manual*** for instruction necessary to operate the equipment safely in accordance with its function and intended use.

## Document Conventions

This manual uses the following conventions.

### Typographical Conventions

Convention	Description
<b>Bold Text</b>	Indicates keys on the keyboard, text to enter, or hardware items such as buttons or switches on the equipment.
<b><i>Italicized-Bold Text</i></b>	Indicates software terms that identify menu items, buttons or options in various windows.
<b>CTRL+ESC</b>	Indicates a keyboard operation. A plus (+) sign between the names of two keys indicates that while holding the first key, you should press and release the second key. For example, Press <b>CTRL+ESC</b> means to press and hold the <b>CTRL</b> key and then press and release the <b>ESC</b> key.
<b>&lt;space&gt;</b>	Indicates that you must press the spacebar. When instructions are given for typing a precise text string with one or more spaces, the point where you must press the spacebar is indicated as <b>&lt;space&gt;</b> . This ensures that the correct number of spaces is inserted in the correct positions within the literal text string. The purpose of the < > brackets is to distinguish the command from the literal text within the string.

Convention	Description
<b>Enter</b>	Indicates that you must press the <b>Enter</b> or <b>Return</b> key on the keyboard. Do not type <b>Enter</b> .
>	<p>The greater than symbol, or right angle bracket, is a concise method to indicate a sequence of menu selections.</p> <p>For example, the statement "From the main menu, select <b>System</b> &gt; <b>Setup</b> &gt; <b>Options</b> to open the <b>Option Activation</b> window" replaces the following:</p> <ol style="list-style-type: none"> <li>1. From the main menu, select <b>System</b> to open the <b>System</b> menu.</li> <li>2. From the <b>System</b> menu, select <b>Setup</b> to open the <b>Setup</b> menu.</li> <li>3. From the <b>Setup</b> menu, select <b>Options</b> to open the <b>Option Activation</b> window.</li> </ol>

## Illustrations

All illustrations in the manual are provided as examples only. Depending on system configuration, screens in the manual may differ from the screens on your system.

All patient names and data are fictitious. Any similarity to actual persons is coincidental.

## Notes

Notes provide application tips or additional information that, while useful, are not essential to the correct operation of the system. They are called out from the body text through a flag word and indentation, as follows:

**NOTE:**

The tip or additional information is indented below the **NOTE** flag word.

## Related Documents

The following documents provide additional information that may be helpful in the installation, configuration, maintenance, and use of this system.

### Documents Related to the MUSE Cardiology Information System Service Manual

Part Number	Document Title
2034539-042	MUSE Cardiology Information System Operator's Manual
2034539-172	MUSE Cardiology Information System Hardware Manual
2034539-044	MUSE Cardiology Information System Pre Installation Manual
2034539-180	MUSE Cardiology Information System Devices and Interfaces Manual
2034539-050	MUSE Cardiology Information System Client Installation Manual
2020299-021	MobileLink Wireless Communication Installation Manual
2020299-025	LAN Option for MAC Resting ECG Systems Installation and Troubleshooting Guide
2034539-048	MUSE Cardiology Information System Advanced Security Guide

# Product Overview

This chapter provides a general description of the product, its connectivity to other devices and interfaces, and a description of available options.

## General Operation

The MUSE system consists of an application/database server that stores the system configuration and patient tests (ECG, Stress, Holter, and HiRes) in a relational database.

Client computers run the MUSE application and communicate with the MUSE database via a middle-tier service that runs on the MUSE server.

Depending on the device and the system configuration, you can acquire tests over a:

- wired network
- wireless network
- modem
- floppy diskette
- secure digital (SD) card
- serial download cable
- any combination of these

You acquire the tests from associated devices for a particular type of study. These data types come from devices or systems such as:

- ECG Electrocardiograph Carts
- CASE Stress systems
- MARS Holter systems
- Patient monitors

The MUSE application connects client workstations to the server over the network. These workstations access the server to perform system functions such as editing, test retrieval, system setup, running database searches, and checking system status.

The editor application allows you to complete overreading, retrieving, and confirming tests. You can manually or automatically route the tests to output devices such as laser printers, network laser printers, fax machines, an HL7 (Health Level 7) interface, or to destinations such as email addresses and shared folders. You can manually or automatically route the tests to output devices such as shared printers, fax machines, an HL7 Results device, or to destinations such as e-mail addresses and shared folders.

## Data Acquisition

You can acquire data into the MUSE system database from several different interfaces and data sources. Following is a summary of the different interfaces:

- **CSI**  
ECG carts send data either through a serial cable connected to a workstation, a CSI modem, a 802.11b/g wireless connection, or through a LAN connection.
  - **Direct Media Acquisition**  
The MUSE system can acquire data that was stored to local media on an ECG cart, such as a floppy disk (on older carts), or a Secure Digital (SD) card.
  - **General Acquisition**  
The MUSE system can acquire data from either a local folder or from a network share. Use this method to acquire data from bedside monitors, MARS Holter systems, and CASE stress systems. The MUSEBkgnd account being used to run the MUSE services needs access to the folder in order to acquire the data.
- NOTE:**  
MUSE v8 does not support acquiring new patient data from CASE systems running Windows NT or older operating systems.
- **XML Import**  
You can send ECG data from other vendor devices to the MUSE system through the XML Import feature, which is a purchasable option. MUSE supports the XML format sent from the LifePak®12/15 defibrillators, DatamedFT® format translator software, and Getemed Cardioday® Holter\ECG system.

Data acquired at a workstation is copied through the network to the MUSE server for processing and storage. Depending on the type of test, the size of the acquired data varies. Acquired data is placed in the **Newly Acquired Queue** in the database. From there the system processes the data into the system and makes it available to users for viewing, editing, or printing. You can automatically route tests to MUSE-defined devices upon acquisition into the system, when saved as **Demographics Complete**, or when confirmed by an overreader. The following Data Types table lists the different data types you can store on the MUSE system, along with the acquisition device, and typical record size.

### Data Types

Data Type	Acquisition Device	Typical Record Size
Resting ECG — 12 Lead (250 Hz)	Electrocardiograph	7 KB
Resting ECG — 12 Lead (500 Hz)	Electrocardiograph	10 KB — 20 KB
ECG (240 Hz)	Clinical (monitoring) device	7 KB
Hi Resolution ECG — 15 Lead	Electrocardiograph	10 KB — 20 KB
Stress	CASE	750 KB — 3 MB
Holter	MARS	1 MB — 2.5 MB

## Device Interfaces

The MUSE system can interface with the following systems and devices:

- MAC Carts
- MARS
- CASE/CardioSoft Stress Systems
- Monitoring Systems

## MAC Carts

You can send ECG data acquired at the MAC carts into the MUSE system for long-term storage. Depending on the type of cart and the options installed, you can send data one of several ways:

- Remove the diskette or secure digital (SD) card from the cart and download it onto a MUSE client
- CSI modem
- CSI direct (direct serial connection)
- CSI network (wireless/LAN)

Carts supporting Remote Query allow the cart to retrieve a record from the MUSE system. You must purchase Remote Query as a cart option. The Advanced Security features that are part of the MUSE software allow you to turn off Remote Query on a per-site basis within the MUSE system.

The following table provides the methods available for transferring data from the Cart to the MUSE system. Many of the methods listed require the purchase and activation of an option on the cart. Refer to your GE Healthcare sales representative for more information.

### ECG Cart Interfaces to MUSE

ECG Cart	CSI Modem	CSI Network		CSI Direct	Diskette	SD Card	Remote Query
		Wireless	LAN				
MAC 600				X		X	
MAC 800	X		X	X		X	
MAC 1200	X			X			
MAC 1600	X		X	X		X	
MAC 3500	X	X <sup>1</sup>	X	X		X	
MAC 5000	X	X		X	X		X
MAC 5500	X	X	X	X		X	X

<sup>1</sup>This option is available on the MAC 3500 only outside of North America.

## MARS

You can configure MARS Holter systems to store saved reports to the MUSE system for long-term storage. **Full Disclosure** is not sent to the MUSE system. To accomplish the data transfer, the MUSE system connects to a network share on the MARS system over the network and copies the files to the MUSE application/database server for processing. The MUSE system requires the **Holter Data Type** option. UNIX-based MARS systems require the enterprise network card option.

## CASE/CardioSoft Stress Systems

You can configure the CASE/CardioSoft Stress systems to store saved reports to the MUSE system for long-term storage. CASE/CardioSoft systems require a network option to send data to the MUSE. The CASE/CardioSoft system copies the files to a shared folder on the MUSE system, and then the MUSE system picks up the files locally for processing. You must enable the **Exercise Testing** option for the MUSE system.

## Monitoring Systems

You can configure bedside monitors to send 12-lead ECG data to the MUSE system for long-term storage. You accomplish this through the use of a monitoring gateway, which is a computer that has two network interfaces: one on the monitoring network, and one on the hospital network on which the MUSE application/database server is located. When you send a test to MUSE from a bedside monitor, the monitoring gateway receives it and stores it locally in a shared folder. The MUSE server is configured to look for data on that network share, and when it finds new data, moves it to the MUSE server and processes into the system.

## Modems

The MUSE system uses modems to receive and send data to carts and to fax reports from the MUSE system.

### Modem Types

The following table describes the types of modems the MUSE system uses:

#### Modem Types

Type	Usage	Where Installed
CSI	Receive/Send with ECG cart	Normally installed on the server, but a workstation can support it based on the location of phone lines and the need to avoid long distance calls.
FAX	Send to fax machine	Normally installed on the server, but a workstation can support it, based on the location of phone lines and the need to avoid long distance calls. Older Fax modems are installed on the SMM client only.

If you purchase a GE Healthcare-supplied modem, you receive the MultiTech MT9234ZBA modem. For detailed information about the MultiTech modem, refer to the **MUSE Cardiology Information System Hardware Manual**.



## CSI Modem

The CSI modem is an external modem connected to the MUSE server or a MUSE client. It can communicate with the following ECG carts:

- MAC 800
- MAC 1200
- MAC 1600
- MAC 3500
- MAC 5000
- MAC 5500

CSI is a proprietary protocol running on top of Serial Line Internet Protocol (SLIP) and does not include the ability to respond to standard IP network connections, such as PING.

CSI modems are typically used to send ECGs to the MUSE system from a cart, but you can also use them to send tests or orders back to the cart.

There are no security risks associated with this modem. The CSI protocol does not respond to IP-based probing, and does not allow any access to system processes or the file structure. Someone with a cart having the Remote Query option could retrieve an ECG if they knew the phone number of the system. You can disable this functionality on the system if you use the MUSE Advanced Security Options.

## Fax Modem

The fax modem uses Class II Group 3 faxing, at 9600 Baud.

The fax modems on MUSE systems are output only and do not accept incoming calls. It is impossible for anyone to access the MUSE system by calling into a fax modem.

When setting up a fax modem, determining the appropriate location is important regarding fax modem location relative to area codes. For instance, a remote hospital sharing the same MUSE server, faxing records locally, would be better served by adding a fax modem on a local computer to reduce phone costs.

There are no associated security risks with this modem since it does not accept incoming calls and cannot access the MUSE system.

## Multi-port Modem Card

You can equip the MUSE server with a multi-port serial adapter. GE Healthcare provides the Digi AccelePort® 8-port PCI adapter (Digi part number 77000889), which can connect eight, DB9 connections to support up to eight modems. Serial ports are configured for COM 3 – COM 10.

## HL7 Interface

The MUSE system supports HL7 interfaces to exchange ADT, Order, Result, and Billing messages between the MUSE server and the Hospital Information System (HIS). You must purchase and enable the appropriate HIS option (ADT, Orders, Results, Billing, ADT Query, Batch Processing) for the MUSE system.

The following software is installed by GE Healthcare service during installation:

- HL7 Interface software
- Adobe Acrobat Reader

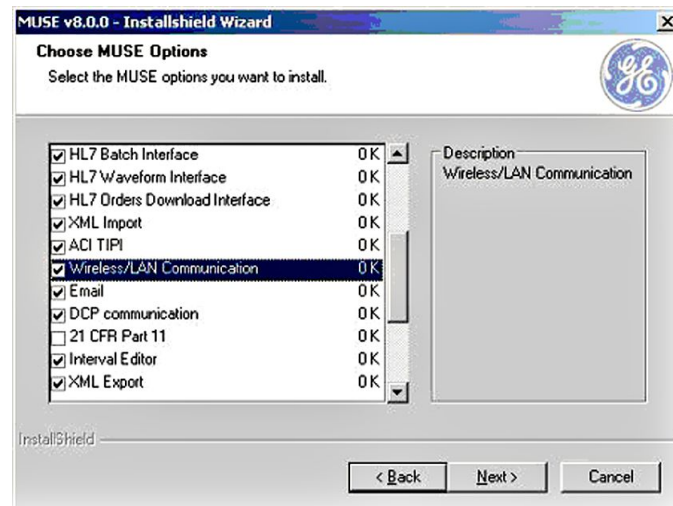
Both the MUSE application and SQL 2005 (single user license) are installed on the HL7 server for configuring and testing of the HL7 interface with the Hospital Information System during initial system installation. These applications are not needed for operation of the HL7 interface and you may remove them from the production HL7 server after installation and testing are completed.

**NOTE:**

GE Healthcare configures a weekly backup of the HL7 configuration as a Windows scheduled task called **SystemState\_Recurring\_Backup**. This scheduled task saves the configuration to the **c:\SystemState** folder. You can use this backup to restore the HL7 configuration. The customer is responsible for making a copy of this folder and saving it to a network drive or external media.

## Optional Features

To view a list of installed options on the system, run the MUSE v8 application in **modify** mode and view the MUSE Options screen. Refer to [“Modifying the MUSE Installed Configuration” on page 58](#) for information regarding running in **Modify** mode.



**CAUTION:**

**SYSTEM FAILURE:** Running in modify mode exposes critical MUSE system configuration settings. Unintended or poorly implemented changes to the MUSE configuration can result in the MUSE system failing.

Do Not launch the MUSE system in modify mode unless you are trained and understand how your changes affect the MUSE system.

The following features are standard on all MUSE v8 systems:

- Database Search
- ACI TIPI

- Wireless/LAN communication
- HiRES Data Storage

**NOTE:**

The MUSE options listed in the following table can only be installed by an authorized GE Healthcare service representative.

The following table lists available options.

**System Features Options**

Purchased Option	MUSE Option(s) Installed	Description
Stress Module	Exercise Testing Data Storage	Includes: <ul style="list-style-type: none"> <li>• LAN interface to CASE Exercise Systems</li> <li>• Ability to edit discreet data and report elements</li> <li>• Ability to view saved strips from CASE</li> <li>• Ability to attach orders if you are using the MUSE HL7 HIS Orders option</li> </ul>
Holter Module	Holter Data Storage	Includes: <ul style="list-style-type: none"> <li>• LAN interface to MARS Holter Systems</li> <li>• Ability to edit discreet data and report elements</li> <li>• Ability to view saved strips from MARS</li> <li>• Ability to attach orders if you are using the MUSE HL7 HIS Orders option</li> </ul>
ECG Serial Comparison	Serial Comparison	<ul style="list-style-type: none"> <li>• Provides automatic comparison to identify clinically significant changes in the current ECG to the first previous ECG</li> <li>• Using GE Marquette 12SL ECG analysis statements</li> <li>• measurements for QRS, ST</li> <li>• morphology changes</li> </ul>
Enhanced ECG Editor	Enhanced Editor	Includes: <ul style="list-style-type: none"> <li>• full screen views for 12/15-lead adult/pediatric ECG and HiRes ECG</li> <li>• Serial Presentation for current, first previous, and oldest ECGs</li> <li>• Magnification, March-out Calipers, and Serial Comparison On—Demand</li> </ul>
ECG Reanalysis	Re-analysis	Reanalyses incoming ECG tests with the latest version of 12SL algorithm software.

## System Features Options (cont'd.)

Purchased Option	MUSE Option(s) Installed	Description
Third party XML Import Interface	XML Import	<ul style="list-style-type: none"> <li>Provides capability for automated acquisition and report routing of ECGs from multi-vendor devices or system utilizing XML formatted data.</li> <li>Supports Physio-Control LIFEPAK and Getemed CardioDay ECGs, as well as 12-lead ECG data sent to the MUSE system through the DatamedFT software.</li> </ul>
Third-party XML Export Interface	XML Export	Provides <ul style="list-style-type: none"> <li>10-second 12/15-lead ECG data</li> <li>patient demographics</li> <li>test information</li> <li>global measurements QRS times and types</li> <li>Automated single record or bulk transfer in XML format for external systems</li> </ul>
21 CFR Part11 Module (for FDA Guidelines)	21 CFR Part 11	Provides: <ul style="list-style-type: none"> <li>audit trail</li> <li>electronic signature</li> <li>password prompt on confirmation</li> <li>reason for change</li> <li>enumerated list or free text</li> <li>logging changes to ECG and subject data</li> <li>user-definable text for signoff</li> </ul>
ECG Interval Editor Module	Interval Editor	Provides: <ul style="list-style-type: none"> <li>beat-by-beat raw or median beat editing</li> <li>Automated recalculation including global and lead-by-lead QT interval calculations</li> <li>Semi-automated and manual modes</li> <li>Trial setting lock-down</li> <li>E14 tools</li> </ul>
FDA Format XML Export Interface	XML Export	Provides ECG data export in FDA format
CV Web 2.0	MUSE API (MACCRA) and MUSE Web	Provides online access to the MUSE v8 system via a secure online URL link to retrieve and view ECG, stress, and Holter reports.
VA VistA Image Interface	MUSE API (MACCRA) and MUSE Web	Provides result link to VA VistA Image display system
MUSE Web Connectivity to GE Healthcare Devices	MUSE API (MACCRA) and MUSE Web	Provides web interface to GE Healthcare devices, such as CASE and Panel.
Email Module	Email	Provides distribution of MUSE reports to customer email systems

## System Features Options (cont'd.)

Purchased Option	MUSE Option(s) Installed	Description
ADT Module	ADT Interface	Receives admission, discharge, and transfer information from facility ADT provider (for example HIS).
Orders Module	HL7 Orders Download Interface HIS Orders Interface	<ul style="list-style-type: none"> <li>Receives orders from facility order entry system</li> <li>Provides ability to download order information to selected MAC carts and CASE stress systems configured with MUSE connectivity</li> <li>Requires ADT</li> </ul>
ECG/Stress/Holter Text Results Module	HL7 Results Interface	Sends ECG, stress, or Holter textual results to facility Electronic Medical Record system.
Waveform Image Results Module	HL7 Waveform Interface	<ul style="list-style-type: none"> <li>Sends waveform results to facility Electronic Medical Record system.</li> <li>Requires ECG/Stress/Holter Text Results module.</li> </ul>
ADT Query Module	HL7 ADT Query Interface	<ul style="list-style-type: none"> <li>Queries admission, discharge and transfer information from facility ADT provided (for example HIS).</li> <li>Requires ADT.</li> </ul>
Billing Module	HL7 Billing Interface	Provides real-time transfer of financial transaction information to facility HIS.
Batch Data Module	HL7 Batch Interface	<ul style="list-style-type: none"> <li>Transfers textual results or financial transaction information in batch mode to facility HIS.</li> <li>Requires Billing.</li> </ul>

## Hardware Specifications

For hardware requirements, refer to the ***MUSE v8 Cardiology Information System Pre Installation Manual***.

For information regarding replacement parts for GE Healthcare-supplied hardware, refer to the ***MUSE Cardiology Information System Hardware Manual***.

## Software Specifications

For information regarding software requirements and specifications, refer to the ***MUSE Cardiology Information System Pre Installation Manual***.

## The MUSE System in Virtual Environments

Customer-supplied virtual machines must meet or exceed the virtual hardware requirements described in the MUSE v8 Cardiology Information System Pre-Installation Manual. Software requirements (operating system and service packs) remain the

same as those for a physical server. GE Healthcare reserves the right to request the virtual machine's virtual hardware configurations and to request allocation of additional CPU or memory to resolve performance-related issues.

## Customer Responsibilities

The following are customer responsibilities when operating the MUSE system in a virtual environment:

- Completion of the setup and configuration of the virtual machine(s) on which the MUSE system is being installed prior to the arrival of the GE Healthcare installation engineer.
- Completion of a MUSE database backup and recovery plan, including its implementation and testing.
- Contact with the VM software vendor to resolve issues specific to the virtual environment.

GE Healthcare service engineers support the MUSE system running on the Windows operating systems as stated in the MUSE v8 Cardiology Information System Pre-Installation manual, regardless of whether that operating system is installed on a physical or virtual machine. However, GE Healthcare does not provide support for installation or configuration of the virtual environment, or any feature set provided as part of that environment, such as high availability, fail-over clusters, or SAN.

## Data Acquisition

CSI modems, used to acquire data from some MAC carts, cannot connect directly to a virtual MUSE server, but can connect to a MUSE client.

## HL7 Interface Virtual Machine

The software used for the HL7 interface is a multi-threaded application and is optimized for use with two CPUs. The use of only one CPU affects performance and slows down transaction processing.

## Licensing

The software used to run the HL7 interface is licensed using the MAC address of the server. Any change to the MAC address within the virtual machine causes the interfaces to fail.

## MUSE v8 Drive Contents and Supporting Folders

The following drive letters are the recommended installation configurations. MUSE supports installation on other drive partitions.

## Muse Application and Database on Same Server

This is the simplest configuration and avoids the need to adjust firewall settings and set permissions between the MUSE server and SQL databases. It is the standard configuration when MUSE is installed on GE Healthcare-supplied servers.

### C: Drive

Application	Description
Windows OS	
Adobe Reader 9	
SQL Server 2005	
SQL Management Studio	
MUSE	MUSE application folder located in Program Files
InSite ExC	Enables GE Healthcare remote support

### D: Drive (MUSE)

Folders	Description
db	MUSE databases
acq	Network share to temporarily store ECGs being acquired from MARS and Monitoring Gateway
backup	Supporting files for GE Healthcare tape or network backup
mars	Temporarily stores formatted Holter reports ready for printing
xml	Temporarily stores inbound xml data (requires XML import option)

## MUSE Application and Database on Separate Servers

### MUSE Application Server

Application/Folders	Description
Windows OS	
Adobe Reader 9	
SQL Server 2005	
SQL Management Studio	Required for access to MUSE database
MUSE	MUSE Application folder located in Program Files
InSite ExC	Enables GE remote support
MUSE data folder	The name and location of the MUSE data folder is specified during MUSE system installation. In a typical installation, the folder name is <b>MUSE</b> and includes the following folders:
\acq	Network share to temporarily store ECGs being acquired from MARS and Monitoring Gateway

## MUSE Application Server (cont'd.)

Application/Folders	Description
\backup	Supporting files fro GE tape or network backup
\mars	Temporarily stores formatted Holter reports ready for printing
\xml	Temporarily stores inbound xml data (requires XML import option)

## MUSE Database Server

Application/Folders	Description
SQL Server 2005	
muse\db	MUSE Databases

# MUSE Services

MUSE uses a group of services to perform certain functions within the MUSE application. Services are installed to use the default **MuseBkgnd** as the logon account. This account requires **sysadmin** privileges to the MUSE databases.

The following table provides a list of MUSE services with a brief description of each. When troubleshooting specific problems, it is sometimes useful to verify that the corresponding service is running.

### CAUTION:

STOPPING A SERVICE DISABLES THAT FUNCTION: Do not stop services unless you understand how it affects the system, or unless all users are logged off the system.

MUSE v8 includes an **autosshutdown** feature to notify users in advance of a shutdown. Refer to [“AutoShutdown” on page 56](#) for more information on using **autosshutdown**.

## MUSE Services

Service	Description
MUSE SCM	Service Control Manager: turns all MUSE services off and on
MUSE Email	Handles email transmission
MUSE File Copy	Copies output to folder devices
MUSE format	formats output to MUSE devices other than HL7
MUSE FTP Copy	copies output to FTP folder devices
MUSE Generic	Acquires Hilltop data from shares (ECG, Stress, and Holter)
MUSE HL7 Outbound	supports Outbound Results and/or Billing
MUSE HL7 Parser 1–4	Supports individual inbound feeds FROM Hospital Information System (HIS)



## MUSE Services (cont'd.)

MUSE Print	Handles printing to PS and PCL printer devices
MUSE MACCRA	Supports MUSE Web and MUSE API
MUSE modem	Supports CSI, Fax, LAN, and wireless communication
MUSE MT Host	Handles Middle Tier communications between the client and server
MUSE Normal	Normalizes acquired ECGs
MUSE Scheduler	Runs MUSE scheduled tasks: database search, SQL jobs, log and queue maintenance
MUSE XML Parser	Supports XML acquisition

## Required Network Ports

The following port information for the MUSE system is provided as a guideline to help you understand the system's networking requirements and to assist in situations where you may need to consider either software or hardware firewall configurations. Not all systems use each connection. The ports listed are default values and in some cases can be changed.

### Networking Ports

Purpose	Port	Type	Notes
General Acquisition	137	UDP	Required to exchange data via a network share or with external sources, such as a MARS system or Monitoring Gateway. If <b>NetBIOS over TCP/IP</b> is disabled, only port 445 is required.
	138	UDP	
	139	TCP	
	445	TCP	
SQL Server	1433	TCP	Listens for incoming connections. Can be changed.
	1434	UDP	Allows administrators to check the status of SQL databases. These ports must be open to the MUSE server.
MUSE Application	8001	TCP	Default port used by MUSE user interface applications (Editor, Setup, Status, Database Search). You can change this port, but it must be the same on both the MUSE servers and clients.
MUSE Web	80	TCP	Port 80 is the default port for HTTP traffic. You may change this in the Web Site properties.
CSI Network	3001	TCP	The MAC carts use when transmitting data to the MUSE system over LAN or wireless. This port can be changed.
Remote Support	443	TCP	InSite ExC uses this to communicate with GE Healthcare support.



# System Setup

This chapter provides additional instructions for configuration of the MUSE system after installation is complete.

## Setting Up Modems

The MUSE system uses the following modems to send and receive data:

### MUSE Modem Types

FAX Modem	Supports outgoing fax transmissions
CSI Modem	Supports cart modem connections for data upload, order download, and reverse transmission to a cart
CSI Direct	Supports direct serial cable cart connections
CSI Network	Supports wireless and/or LAN cart connections

To support any of the available modems on MUSE v8.0, the **MUSE Modem** feature must be installed and the **MUSE Modem** service must be running.

#### NOTE:

During the upgrade from an earlier version of MUSE to MUSE v8.0, all CSI Wireless modems were converted to CSI Network modems. If you see a CSI Wireless entry in the **Modem Setup** list, the modem server for that modem was not upgraded or it is missing. In a normal situation, you should never see a CSI Wireless device after upgrading to MUSE v8.0.

## Verifying/Installing the MUSE Modem Service and Wireless/LAN Communication

#### NOTE:

Muse options can only be installed by an authorized GE Healthcare service representative.

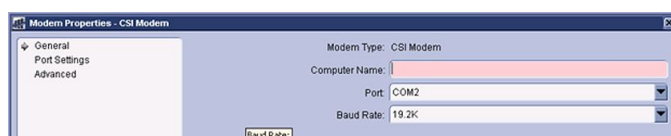
Use the following instructions to verify and install the MUSE Modem service and wireless/LAN communication.

1. Run the **MUSE Installer** in **Modify** mode. See [“Modifying the MUSE Installed Configuration”](#) on page 58.
2. On the **Select Features** window, select **Modem**.  
This installs the **MUSE Modem** service. This service is required for modem, as well as, Wireless and LAN transmission.
3. Click **Next** through the following windows until the **Choose MUSE Options** window opens.
4. If you are setting up wireless or LAN communication, verify that the option is selected.  
If you needed to install the option, you are asked on the next screen for the **Option Activation Password**.
5. Enter the password and click **Next** through the remaining windows.  
The **MUSE Modem** service and selected modem option are installed.

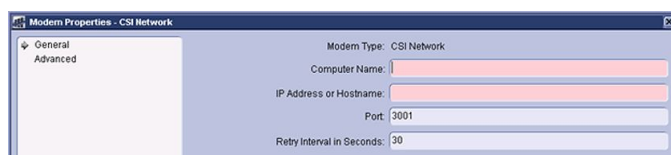
## Setting Up a Modem Device

Use the following instructions to set up a modem device.

1. Log on as a user with privileges to change **MUSE Setups**.
2. Open the MUSE **Setup** application.
3. In the **Navigation** pane, select **Modems**.
4. Right-click in the **Modem** pane, and select **New**.
5. Select the modem type you are adding.  
If you selected **Fax Modem**, **CSI Modem**, or **CSI Direct**, the appropriate **Modem Properties** window opens.



If you selected **CSI Network**, the **Modem Properties — CSI Network** window opens.



6. Enter the appropriate values described in the following tables.

#### Fax, CSI, or CSI Direct Modem Properties

Field	Description
<b>Computer Name</b>	Name of the computer where the modem is physically installed. Typically, this is the MUSE file server.
<b>Port</b>	Port Number
<b>Baud Rate</b>	115.2K Baud (CSI Direct) 9600 Baud (CSI, Fax) <sup>1</sup>
<sup>1</sup> If the Fax modem encounters problems at 9600 baud, use 4800 baud.	

#### CSI Network Modem Properties

Field	Description
<b>Computer Name</b>	Name where the connection is supported.
<b>IP Address or Hostname</b>	The IP Address or Hostname assigned to the cart.
<b>Port</b>	Port this connection is using.
<b>Retry Interval in Seconds</b>	Defines the upper limit of the time delay between attempts for the cart to communicate with the MUSE system. The default is 30 seconds.

7. Select **OK** to save your changes.  
The **Modem Properties** window closes.

#### NOTE:

When a new modem is set up, the **MUSE Modem** service is notified and automatically starts a new thread to support the connection. You do not need to restart the **MUSE Modem** service after defining a new modem.

## Restarting Modems

The individual threads that are running to support each connection are designed to automatically restart if they stop for some reason. Use the following procedure if you want to restart them manually:

1. Select **SetupModems**.
2. Select the modem(s) that you want to restart, right-click on it, and select **Restart Modem**.



**NOTE:**

There is also a restart modem icon on the toolbar.

A message displays that the modems were successfully restarted.



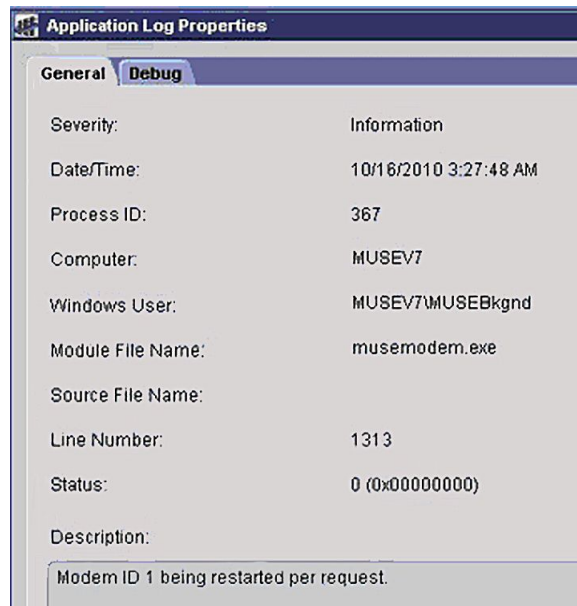
**NOTE:**

If you do not receive this message, the **MUSE MT Host** service was not able to communicate to the **MUSE Modem** services. There are two causes for this:

- The **MUSE Modem** service is not running.
- The firewall settings on the **MUSE Modem** service's host system are not configured correctly.

3. For more information about the modems, when they start or restart, select **Status > Application Log**.

The **Application Log Properties** window opens



If the connection to a cart fails, the **MUSE Modem** service immediately attempts to restart it. The failure and restart are logged in the **Application Log**.

If the restart fails within one minute, the service does not wait until the one minute interval is up before trying again.

If there are three consecutive failures within one minute, a message is logged indicating that error message logging for this modem is stopped until the modem is working again. This prevents the **Application Log** from filling up with repetitive error messages. While no messages are being logged, the service continues to restart the modem in the background. Once the modem is restarted and continues running for at least one minute, logging resumes for this modem. Manually restarting the modem from the user interface also resumes logging.

## Testing CSI Network Modem Connections

Use the following procedure to view the connection status for each network connection.

1. Open a **Command Prompt** window.
2. Type **netstat <space> -n**.

This displays a list of all open socket connections on the system.

If a connection is established between the **MUSE Modem** service and the cart, there is an entry containing the local address with the IP address of the server, the foreign address with the IP address of the cart, and the port number after the cart's IP address.

Protocol	Local Address	Foreign Address	State
TCP	3.62.92.2:61226	3.159.18.49:2002	ESTABLISHED
TCP	3.62.192.148:3001	3.62.192.148:52379	ESTABLISHED
TCP	3.62.192.148:52379	3.62.192.148:3001	ESTABLISHED
TCP	127.0.0.1:3000	127.0.0.1:52381	ESTABLISHED
TCP	127.0.0.1:52372	127.0.0.1:3000	TIME_WAIT
TCP	127.0.0.1:52381	127.0.0.1:3000	ESTABLISHED

Item	Description
1	Server IP address
2	Cart IP address*
3	Port Number
4	Connection state
*In this example the cart is a simulator running on the same system. Normally the server and cart are not the same IP address.	

If the cart is not connected, you do not see an entry in this list. The MUSE Modem service opens a connection once the number of seconds equal to the retry interval is reached. If it fails to connect, it closes this connection until the next interval time.

## Installing and Configuring the XML Import Option

The XML Import option is required for systems that are acquiring data in XML format. The MUSE system can acquire data in XML format from the following devices:

- LifePak 12 through the LIFENET Receiving Station (reference document 2002783-040).
- From a Datamed FT (Format Translator) provided by Engineering Solutions, Inc.
- CardioDay Holter ECG System.

XML Import requires that the **XML Import** option and the **MUSE XML** service are installed on the MUSE application serve as follows.

**NOTE:**

MUSE options can only be installed by an authorized GE Healthcare service representative.

## Installing the XML Import Option and MUSE XML Service

Use the following procedure to install the **XML Import** option and **MUSE XML** service

1. Run the **MUSE Installer** in **Modify** mode. See [“Modifying the MUSE Installed Configuration” on page 58.](#)
2. On the **Select Features** window, select **XML**.  
This installs the **MUSE XML Parser** service.
3. Click **Next** on each of the next windows until the **Choose MUSE Options** window opens.
4. Verify that the **XML Import** option is selected.  
If you needed to install the option, you are asked on the next screen for the **Option Activation password**.
5. Enter the **Option Activation password**.
6. Click **Next** on each of the remaining windows.  
The **XML Import** option and **MUSE XML Parser** service are installed.

## Requirements

XML Import requires **MSXML 4.0**. This program should have been installed during the initial MUSE installation.

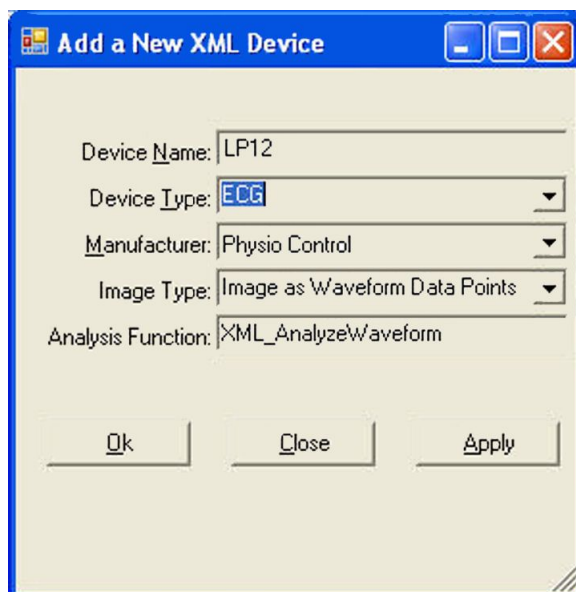
## Using XMLCONFIG.EXE to Configure the Option on MUSE

This utility inserts entries into the **cfgXmlInput** table in the **MUSE\_System** database.

1. Run the **xmlconfig** utility located in the folder where the MUSE application is installed, typically **C:\Program Files\MUSE**.
2. Click **New Device**.



3. Set the correct options for the appropriate device.  
For **LifePak 12** enter/select the following:



The screenshot shows a Windows-style dialog box titled "Add a New XML Device". It contains the following fields and controls:

- Device Name:** A text box containing "LP12".
- Device Type:** A dropdown menu with "ECG" selected.
- Manufacturer:** A dropdown menu with "Physio Control" selected.
- Image Type:** A dropdown menu with "Image as Waveform Data Points" selected.
- Analysis Function:** A text box containing "XML\_AnalyzeWaveform".
- At the bottom, there are three buttons: "Ok", "Close", and "Apply".

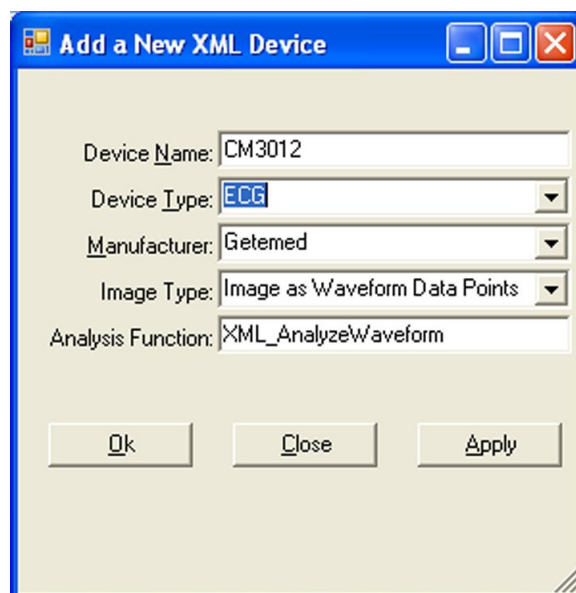
For a **DatamedFT**, enter/select the following:



The screenshot shows a Windows-style dialog box titled "Add a New XML Device". It contains the following fields and controls:

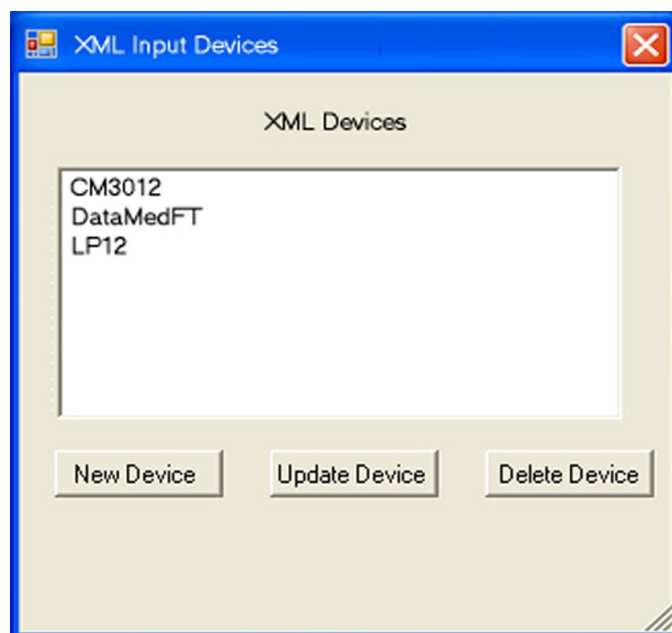
- Device Name:** A text box containing "DataMedFT".
- Device Type:** A dropdown menu with "ECG" selected.
- Manufacturer:** A dropdown menu with "DataMed" selected.
- Image Type:** A dropdown menu with "Image as Waveform Data Points" selected.
- Analysis Function:** A text box containing "XML\_AnalyzeWaveform".
- At the bottom, there are three buttons: "Ok", "Close", and "Apply".

For **Getemed C3012**, enter or select the following:



The screenshot shows a Windows-style dialog box titled "Add a New XML Device". It contains five input fields: "Device Name" with the text "CM3012", "Device Type" with a dropdown menu showing "ECG", "Manufacturer" with a dropdown menu showing "Getemed", "Image Type" with a dropdown menu showing "Image as Waveform Data Points", and "Analysis Function" with the text "XML\_AnalyzeWaveform". At the bottom of the dialog are three buttons: "Ok", "Close", and "Apply".

4. Click **Ok**.
5. Create other devices, update an existing device, or delete a device as required.



The screenshot shows a Windows-style dialog box titled "XML Input Devices". It has a list box labeled "XML Devices" containing the text "CM3012", "DataMedFT", and "LP12". Below the list box are three buttons: "New Device", "Update Device", and "Delete Device".

6. When you are finished, click the **close box (X)** to exit the utility.

## Setting Up the MUSE File Server for File Copy

This section describes how to set up a **File Copy Device**. Use this if you want to copy an ECG to a folder on the MUSE file server or to a network share.

You must install the **MUSE File Copy** service to use this feature. This service is normally installed with all MUSE v8 systems and is initially set up to use the same service logon account (**MUSEBkgnd**) that all MUSE services use.

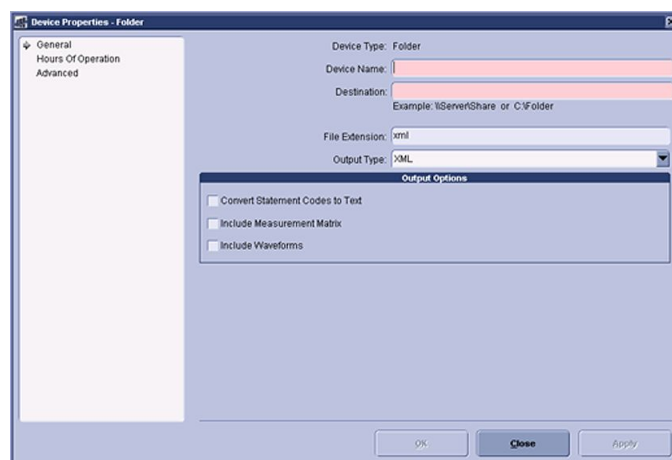
If you are sending files to another computer on a domain, you need to use **domain\MUSEBkgnd** as the logon for the **MUSE File Copy** service. If the MUSE services were originally installed to use a local **MUSEBkgnd** account, you need to change the logon service for the **MUSE File Copy** service. Work with the hospital network administrator to create a **domain\MUSEBkgnd** user account that you can use for the service.

If the MUSE system is installed on Windows 2008, work with the database administrator (DBA) to provide the **domain\MUSEBkgnd** account with **sysadmin** privileges to the MUSE databases.

## Setting Up a Folder

Use the following procedure to set up a folder for **File Copy**.

1. Log on as a user with privileges to change **MUSE Setups**.
2. Open the **MUSE Setup** application.
3. In the navigation pane, click **Devices**.
4. Right-click in the **Devices** pane, and select **New > Folder**.



5. Type the **Device Name** and **Folder Destination** in the appropriate fields.
6. In the **File Extension** field, ensure that the appropriate file extension is displayed.
7. From the **Output Type** drop-down list, select the appropriate file type.
8. Select the appropriate **Output Options**.
9. On the **Hours of Operation** tab, set up the hours of operation for this customer and click **OK**.
10. On the **Advanced** tab, set up the format settings for this customer and click **OK**.

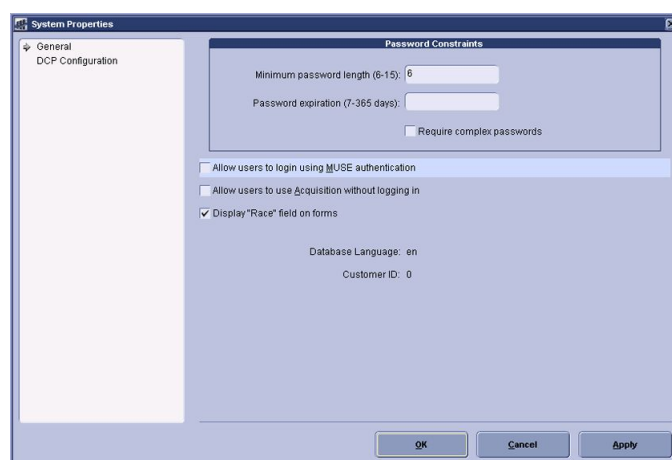
## MUSE Authentication—Enable or Disable

MUSE Authentication is enabled by default during the initial MUSE installation.

Use the following procedure to turn off (disable) MUSE Authentication.

1. Log on to the MUSE application using an account with system setup privileges.
2. Go to **System > Setup**.
3. From the navigation panel, select **System**.
4. Right-click on the name of the MUSE system and select **Properties**.

The **System Properties** window opens.



5. Deselect **Allow users to logon using MUSE authentication**.
6. Click **OK** to save your changes.

## Configuring Windows High Contrast Color Scheme on MUSE Client

For each workstation that may be used by one or more individuals with color vision deficiency (color blindness) you may enable the **Windows High Contrast Color Scheme** for MUSE as follows:

1. From the Windows desktop of the client that is being used by a color impaired individual, select **Start > Control Panel**.
2. Double-click **Display** to open the **Display Properties** window.
3. Select the **Appearance** tab.
4. In the **Windows and buttons** list, select **Windows Classic style**.
5. In the **Color scheme** list, select one of the **High Contrast** options:
  - High Contrast #1
  - High Contrast #2
  - High Contrast Black
  - High Contrast White
6. Click **Apply**.
7. From the Windows desktop, copy a MUSE shortcut icon, which was created during installation, and paste it on the Windows desktop.

8. Rename the shortcut by adding **Windows Default Colors** to the end of the name.
9. Right-click on the shortcut and select **Properties**.
10. In the **Target** field, add the following to the end of the string: **<space> —nocui**.
11. Click **OK** to save your changes.
12. Repeat step 7 through step 11 for each of the MUSE shortcut icons.

**NOTE:**

Inform color impaired system users to use the shortcuts with **Windows Default Colors** appended to the end of the name.

Inform system users who are not color impaired to use the original shortcuts.

## Changing MUSE Service Accounts

The MUSE service accounts are integral to the correct operation of the MUSE system. The following table identifies the default accounts.

To be able to log on to both the MUSE system and Windows, the accounts must be set up with the following user accounts.

### MUSE User Service Accounts

The default **MUSEAdmin** and **MUSEBkgnd** accounts are automatically set up as **Users** within the MUSE application. They are critical to the internal working of the MUSE system and cannot be changed. However, to provide added security, you may modify their passwords. See [“Changing the MUSE User Account Passwords” on page 53](#).

### MUSE Windows User Service Accounts

The Windows **MUSEAdmin** and **MUSEBkgnd** accounts provide access to the MUSE application, MUSE services, and SQL database. They are linked to the MUSE user accounts. While you can change the passwords for the Windows accounts, changing the name of the accounts requires that you change the services and operations dependent on them as well.

## Changing the MUSE User Account Passwords

To change the password of the **MUSEAdmin** or **MUSEBkgnd** account, modify the user's password in the MUSE application.

1. Log on to the MUSE application.
2. Go to **Setup > Users**.
3. Right-click on the account and select **Properties**.
4. From the **User Properties** window, enter a new **MUSE password**.
5. Save your change.



# System Administration

This chapter provides procedures for administrative functions you may need to do on the MUSE system.

## Remote Databases

This section provides additional considerations to ensure MUSE system installation and operation on a remote database. Remote database means that the SQL instance running the MUSE databases is located on a separate server. In a simple MUSE system configuration, the MUSE application, and the SQL and MUSE databases are all installed on the same server.

## SQL Ports

If the MUSE system is using a remote MUSE database, the MUSE application server requires access to the MUSE databases. This requires the following ports be open to the SQL server.

- **SQL Listening Port**  
Listens for incoming connections. For MUSE, these incoming connections originate at the MUSE application server. SQL assigns TCP port 1433 as the listening port when the default instance of SQL is used. If the customer wants added security, they can change this port. When using a named instance of SQL, SQL assigns a dynamic port, which the database administrator (DBA) can change to a known fixed port.
- **SQL Monitor Server**  
The monitor server service uses UDP port 1434, which allows administrators and users to check the status of the SQL databases. Like the listening port described previously, the customer can assign this port a different port number for increased security.

If the MUSE application server is having problems communicating with the database, and the MUSE service accounts have **sysadmin** privileges, contact the local DBA and verify that the correct ports are open.

## SQL Remote Connections

When installed on a separate database, the MUSE application requires that the SQL remote connections are enabled as follows. Contact the local IT department or DBA.

1. On the SQL server, go to **Start > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Surface Area Configuration**.
2. Click **Surface Area Configuration for Services and Connections**.
3. Under the SQL instance where the MUSE databases are being installed, select **Remote Connections**.
4. Verify that the **Local and remote connections > Using both TCP/IP and Name Pipes** check box is selected.  
If it is not selected, select the check box and apply the change.
5. Exit the **SQL Server 2005 Surface Area Configurator**.

**NOTE:**

In addition to the **Remote Connections** configuration, you must start the **SQL Server Browser** service.

## AutoShutdown

The MUSE Autosutdown feature can notify users currently logged on to the MUSE system up to five minutes in advance that it is shutting down.

This feature is only available to MUSE system users who have the **Shutdown** privilege enabled for their role. This privilege is set under **Role > Properties > Setup Privileges**. Roles that have this privilege by default include:

- MUSE Service
- System Owner
- Site Manager

There are two types of shutdown:

- **Full**  
Shuts down ALL MUSE servers, including all HL7 services on the MUSE server. MUSE cannot be launched from a client or from the server.
- **Partial**  
Shuts down MUSE client applications running remotely. The MUSE services continue to run and the MUSE application can be launched at the server.

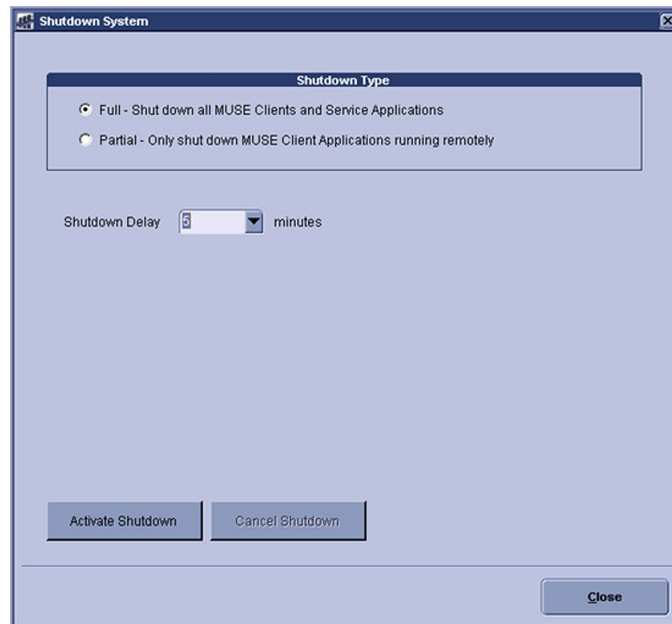
## Activating System Shutdown

Use the following procedure to activate system shutdown.

1. In the MUSE application, go to **System > Setup**.
2. From the navigation pane, select **System**.



3. Right-click on the **Product name** and click **Shutdown System**.  
The **Shutdown System** window opens.



4. Select the **Shutdown Type** and **Shutdown Delay**.
5. Click **Activate Shutdown**.  
A pop-up message opens indicating that the system will be shutting down.
6. Close the message window.  
The top of the MUSE client application displays a countdown.



If you selected a full shutdown, the MUSE client application closes and all MUSE services are shutdown.

If you selected a partial shutdown, all remote connections to the MUSE client application close. The MUSE client application on the server and all MUSE services on the server continue to run.

**NOTE:**

If the MUSE application is still open on remote client, it stops responding and the window automatically closes. Autoshtutdown does not close the application, only its connection to the MUSE server.

## Canceling the System Shutdown

Use the following procedure to cancel system shutdown.

1. Log on to the MUSE application on the server.

**NOTE:**

If the system is in full shutdown mode, manually start the MUSE service. This starts the MUSE MT host service and allows you to log on.

2. The application displays the current shutdown status at the top of the window.



3. In the MUSE application, go to **System > Setup**.
4. On the navigation pane, select **System**.
5. Right-click on the **Product name** and click **Shutdown System**.  
The **Shutdown System** window opens.
6. Click **Cancel Shutdown**.

If the MUSE services were stopped, they are now restarted and remote connectivity is restored.

**NOTE:**

Canceling the shutdown does not automatically notify users that the MUSE system is available.

## Modifying the MUSE Installed Configuration

To view or change the current MUSE installed configuration, run the MUSE v8 Installer in **Modify** mode. The reasons for running in **Modify** mode include:

- Viewing installed options.
- Adding a newly purchased option.
- Adding a service required for a new option.
- Adding a new MARS or Monitoring Gateway system for general acquisition.
- Changing the MUSE Port number.

Before making any configuration changes, read and observe the following cautions.

**CAUTION:**

**LOSS OF DATA:** Changing settings without knowing how they affect the system can result in data loss.

Do not change any current settings unless you understand how the change affects the system.

**CAUTION:**

**LOSS OF DATA:** MUSE Services are designed to restart after making changes to the installation configurations.

To avoid having users lose changes to open records, use the MUSE autosutdown feature to notify users of the shutdown.

Use the following procedure to change an existing configuration.

1. Perform a full or partial shutdown of the MUSE system following the Shutdown procedures described in this manual, or notify users that the system is being shutdown for maintenance.
2. Close the MUSE client application on the server.
3. Go to the **Control Panel**
  - On Windows 2003, open **Add/Remove Programs**.
  - On Windows 2005, select **Classic** view and click **Programs and Features**.
4. Select the **MUSE v8** entry and click **Change**.  
The MUSE InstallShield launches.
5. Verify that **Modify** is selected, and click **Next**.
6. Go through the setup steps and make your configuration changes.

**NOTE:**

You can click **Cancel** at any time to close the program and avoid saving any changes.

7. If no changes are required for a setup window, click **Next** to advance to the next window.
8. The last window to open is **MARS and Monitoring Gateway Connectivity**.

**NOTE:**

Clicking Next at this window IMMEDIATELY applies your changes.

9. Click **Finish**.

If you are adding a service or option, a dialog box displays a message indicating that the services are restarting.



10. After the modifications are complete, cancel the **System Shutdown**.

## Moving the MUSE Databases

Moving the databases requires the assistance and cooperation of the local IT department and database administrator. Contact MUSE Technical Support before performing any database moves. Moving the database consists of the following steps:

1. Preparing the new database server.
2. Detaching and Copying the MUSE databases from the current server.
3. Attaching the databases to the new SQL server.

4. Uninstalling the MUSE application.
5. Reinstalling the MUSE application.

**NOTE:**

You must uninstall and reinstall the MUSE application to establish the new location of the database. Uninstalling the MUSE application also uninstalls MUSE Web. Any customizations that were made to the MUSE Web site need to be reconfigured.

## Preparing the New Database Server

1. Create the SQL instance on which the MUSE application will run.
2. Assign **sysadmin** rights to the **MUSEAdmin** and **MUSEbkgnd** accounts.  
These must be the same accounts that are in the administrators group on the MUSE Application server. The **MUSEBkgnd** account must be the same account that is running MUSE services. Refer to the **MUSE v8 Cardiology Information System Installation Manual** for more information.
3. Create a folder on the SQL server where the databases will be copied.  
While you can use any folder name, it is recommended that you create a **MUSE\db** folder to remain consistent with standard MUSE configurations.

**NOTE:**

For additional information, see [“Remote Databases” on page 55](#).

## Detaching and Copying the MSUE Databases from the Current Server

1. Stop all MUSE services.
2. Open **SQL Server Management Studio** and connect to the current MUSE database server.
3. Expand the **Database** object.
4. Right-click on the **MUSE\_System** database, select **Tasks** and, click **Detach**.
5. On the **Detach Database** window, confirm the name of the database you are detaching and click **OK**.
6. Repeat step 4 and step 5 for each MUSE database. (**MUSE\_SiteXXX**, **MUSE\_Site Template**)
7. Copy the MUSE databases to the new server.

## Attaching the MUSE Databases to the New SQL Server

1. Open **SQL Server Management Studio** and connect to the SQL server where the MUSE databases were copied.
2. Right-click on the **Database** object and select **Attach**.
3. On the **Attach Database** window, click **Add** and browse to the location of the MUSE databases.
4. Select the **MUSE\_System.mdf** file
5. Click **OK** to attach the file

6. Repeat step 2 through step 5 for each MUSE database. (*MUSE\_SiteXXX*, *MUSE\_Site Template*).
7. After all MUSE databases are attached to the new SQL instance, follow the procedures for “Uninstalling/Reinstalling the MUSE Application”.

## Uninstalling/Reinstalling the MUSE Application

Uninstalling the MUSE application removes the following components and entries from the server:

- MUSE directory in Program Files
- MUSE services
- MUSE desktop shortcuts
- MUSE entry in the Start Menu
- MUSE Web folders

The following MUSE components remain on the system:

- MUSE databases (db folder)
- MUSE database subfolders (acq, backup, xml, logs, and so forth)
- .Net Framework
- Adobe Reader
- MUSE Web site (You need to manually remove before reinstalling the MUSE application.

### NOTE:

If you plan on reinstalling the MUSE application later, it is a good idea to run MUSE v8.0 in **Modify** mode and make note of the existing services that are installed.

## Uninstalling the MUSE Application

To uninstall MUSE:

1. Log on to the MUSE application server as administrator.
2. In the **Installed Programs** list, select the **MUSE v8.x** entry.
  - In Windows 2003, click **Start > Control Panel** and select **Add or Remove Programs**.
  - In Windows 2008, click **Start > Control Panel > Classic view > Programs and Features**.
3. Select **MUSE 8.x** and click **Uninstall**.  
MUSE is uninstalled from the system.

## Reinstalling the MUSE Application

Providing that all requirements and permissions for MUSE and MUSE database are met, you can reinstall the MUSE application following the instructions in the **MUSE v8 Cardiology Information System Installation Guide** under the section **Installing the MUSE Application and Database**.

## Renaming the MUSE Server

If the MUSE application is already installed on the sever, use the following procedure to rename the server.

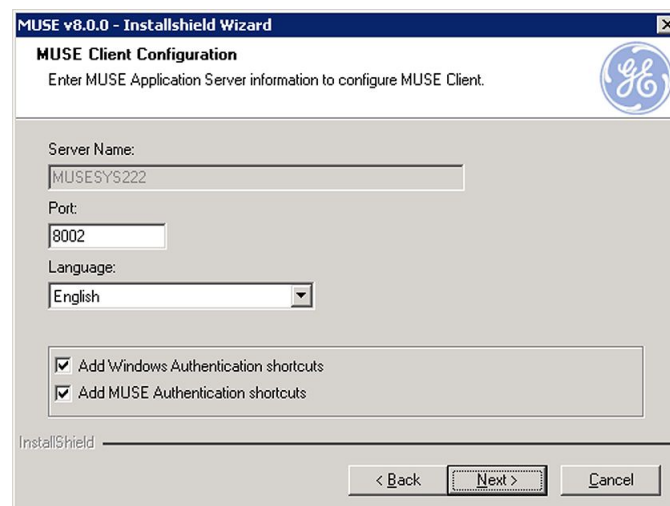
1. Have the local IT or network administrator complete the following steps:
  - a. Rename and restart the server.
  - b. Verify the name change and that the computer has joined the domain.
2. Log on to the MUSE application server as administrator.
3. If SQL is installed on a separate server go to step 4.

If SQL is installed on the same server, rename the local instance of SQL as described in the following steps.

- a. Open **SQL Server Management Studio**.
- b. Connect to the server using the new name.
- c. Click **New Query**.
- d. On the **Query** tab type the following commands
  - **exec sp\_dropserver 'oldname'**
  - **exec sp\_addserver 'newname'**
  - **exec sp\_helpserver**

where **'oldname'** is the old computer name and **'newname'** is the new computer name.

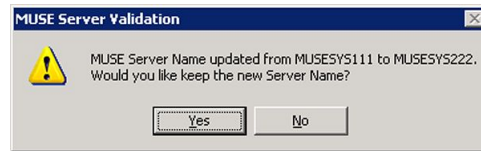
- e. Execute the command and verify that the new name is displayed on the **Results** tab.
4. In the **Installed Programs** list select the **MUSE v8.x** entry.
  - In Windows XP, click **Start > Control Panel** and select **Add or Remove Programs**.
  - In Windows 7, click **Start > Control Panel > Programs and Features**.
5. Select **Modify** and click **Next**.
6. Click **Next** on each window until the **MUSE Client Configuration** window opens.



The new name of the server should be displayed.

7. Click **Next**.

The **MUSE Server Validation** window opens.



8. Click **Yes** to accept the change.
9. Click **Next** on the remaining windows.
10. On the **Maintenance Complete** window, click **Finish**.  
The MUSE services restart.
11. Repeat step 4 though step 10 for each MUSE client.
12. Verify that you can open MUSE on the server and on a client.
13. If MUSE Web is installed on the server, notify users of the new URL.

## Changing the Port Number of the File Server

The port number the MUSE system uses is set during initial installation and you should not need to change it. The port number on all MUSE clients must match the port number set on the server. If a port number change is required, use the following procedure

### NOTE:

Changing the port number causes all MUSE services to restart. Before changing the port number, use the MUSE auto shutdown feature to notify users of the system shutdown.

## Changing the Port Number on the MUSE Server

Use the following procedure to change the port number on the MUSE server.

1. Log on to the MUSE application server as administrator.
2. Perform a System Shutdown. (See “AutoShutdown” on page 56.)
3. In the **Installed Programs** list, select the **MUSE v8.x** entry.
  - In Windows 2003, click **Start > Control Panel**, and select **Add or Remove Programs**.
  - In Windows 2008, click **Start > Control Panel > Classic view > Programs and Features**.
4. Select **MUSE 8.x** and click **Change**.  
The **Welcome** window opens.
5. Select **Modify** and click **Next**.
6. Click **Next** until the **MUSE Client Configuration** window opens.

7. Enter the **port number** you want to use.  
The program checks to see if the port is free. If the port is in use you receive a message.
8. Click **Yes** to continue with the installation using the port entered, or click **No** to go back to the **MUSE Client Configuration** window to change the port number or Cancel the installation.
9. Click **Next** on the remaining windows to save your change.
10. On the **Maintenance Complete** window, click **Finish**.  
The MUSE services restart.
11. After the change is complete, cancel the **System Shutdown**.

## Changing the Port Number on the MUSE Clients

Use the following procedure to change the port number on the MUSE Client.

1. Log on to the MUSE client as administrator.
2. In the **Installed Programs** list, select the **MUSE v8.x** entry.
  - In Windows XP, click **Start > Control Panel** and select **Add or Remove Programs**.
  - In Windows 7, click **Start > Control Panel > Programs and Features**.
3. Select **Modify** and click **Next**.
4. Click **Next** until the **MUSE Client Configuration** window opens.
5. Enter the port number you want to use.  
This must be the same port you configured for the MUSE server. The program checks to see if the Muse server is using the port you entered. If the MUSE server is not using the port you receive a message.
6. Click **Yes** to continue with the installation using the port entered, or click **No** to go back to the **MUSE Client Configuration** window to change the port number or cancel the installation.
7. Click **Next** on the remaining windows to save your change.
8. On the **Maintenance Complete** window click **Finish**.

## BIOS Updates

### Upgrading the G4 Server BIOS Firmware

If you need to replace the 1 MB processor that originally shipped with the G4 application server, you may need to replace it with a 2 MB processor.

**NOTE:**

After replacing the processor, verify if you need to upgrade the BIOS firmware.

You need to upgrade the BIOS firmware if the date displayed when the application server boots is earlier than **11/09/2005 (November 2005)**. If the BIOS firmware date is later, you do not need to upgrade the BIOS firmware.



## Creating a BIOS Upgrade Floppy Disk

You need to create a floppy disk you can use to boot the system.

1. Insert a blank diskette into the floppy drive and the MUSE Support CD into the CD-ROM drive.
2. Select **Start>Run**.  
The **Run** window opens.
3. Click **Browse** and navigate to: **[CD drive letter]:\BIOS\ML370G4\SP31871.exe**.
4. Select the executable and press **Open**.  
The **Run** window is populated with the executable.
5. Click **OK**.
6. Follow the on-screen prompts to create the BIOS upgrade floppy disk.
7. When the process is done, remove the CD from the CD-ROM drive.

## Upgrading the BIOS Firmware

1. Reboot the system with the floppy disk in the drive.  
The system should automatically boot from the floppy disk and display **ROMPAQ Firmware Upgrade Utility V4.20M**.  
**NOTE:**  
If the system does not boot from the floppy
  1. Reboot the system and press **F9** during the boot process.
  2. Select the floppy and the boot drive.
2. At the **Select a Device** window, select **Compaq ML370G4** and press **Enter**.
3. At the **Select an Image** window, select **11/09/2005** and press **Enter**.
4. At the **Caution** window, read and follow the warning: **Do not reboot or turnoff your machine while programming is in process**; press **Enter**.
5. Wait for the upgrade process to complete (2–3 minutes) and display: **Flash Programming Completed Successfully**; press **Enter**.
6. At the message: **Do you want to reprogram another ROM?** press **ESC**.
7. Remove the floppy disk and power cycle the system.



# 5

## Maintenance

A regular equipment maintenance program helps prevent unnecessary equipment and power failures and also reduces possible health hazards. This chapter contains instructions for the following recommended maintenance:

- Cleaning the equipment's accessories
- Visual inspection of equipment
- Exterior cleaning of equipment
- Conducting repair and replacement checkout procedures.

## Maintenance Guidelines

GE Healthcare recommends that you perform the tests described in this chapter:

- Every year as part of routine maintenance.
- Whenever internal assemblies are serviced.
- Whenever you repair or replace equipment.
- As prescribed in the OEM documentation that comes with the equipment.

### **NOTE:**

Unless you have an Equipment Maintenance Contract, GE Healthcare does not assume responsibility for performing the recommended maintenance procedures. The sole responsibility rests with the individual or institution using the equipment. GE Healthcare service personnel may, at their discretion, follow any or all of the procedures as a guide during visits to the equipment site.

Items requiring maintenance include:

- MUSE server(s)
- HL7 Interface Server (CCG)
- MUSE Client
- Monitors
- DVD-RW or CD-RW Drive
- Printer

## OEM Maintenance

For information on maintenance of Original Equipment Manufacturer (OEM) components, please reference the appropriate OEM manuals for the recommended maintenance of their product. For links to the OEM manuals, refer to the **MUSE Cardiology Information System Hardware Manual**.

For technical support, contact your local technical support team.

For technical support, contact your local GE Healthcare technical support team.

## Required Tools and Supplies

In addition to a standard set of hand tools, you need the following special tools and items to maintain or check out the system:

### Required Tools and Supplies

Item	Description
DVOM	Digital Volt/Ohm meter
Leakage Current Tester	used for the Electrical Safety Check
CD-ROM Cleaning Kit	any locally available kt

## Inspection and Cleaning

The equipment is sealed before it leaves the factory. There should be no dust buildup on the surfaces of the interior PCB assemblies and components when you receive it.

If dust is an environmental problem, use a commercially available dust remover (compressed air) to clean the following internal components.

- PCB assemblies
- Cooling fans
- Expansion cards
- Vents

Before beginning any of the following inspection or cleaning tasks, shut down the system and disconnect it from its power source using the appropriate instructions:

- For instructions on shutting down the MUSE system, refer to [“Safe Shutdown Procedures”](#).
- For instructions on shutting down individual components and devices, refer to the appropriate OEM manuals.

# Safe Shutdown Procedures

## Shutting Down the Server

1. Before shutting down the sever, notify all users of the scheduled shutdown.  
For hardware maintenance, do a **Full System** shutdown. (See “AutoShutdown” on page 56.)
2. After the MUSE application is shutdown, then shutdown the server following normal Windows procedures.

## Shutting Down MUSE Client

1. Before exiting the MUSE application, close all patient tests.
2. Close any browser windows or other applications that are open.
3. Shut down the system following normal Windows shutdown procedures.

# Precautions

- Turn off the unit and remove all power before inspecting or cleaning.

### **WARNING:**

**ELECTRIC SHOCK:** Improper use of this device presents a shock hazard. Strictly observe the following warnings. Failure to do so may endanger the lives of the user, and bystanders.

When disconnecting the device from the power line, remove the plug from the wall outlet first, before disconnecting the cable from the device; otherwise, there is a risk of coming in contact with line voltage by inadvertently introducing metal parts in the sockets of the power cord.

Devices may be connected to other devices or to parts of systems only after making certain that there is no danger to the patient, the operators, or the environment as a result. Standards EN/IEC 60601-1-1 must be complied with in all cases.

- Do not immerse any part of the equipment in water.
- Do not drip water or any liquid on the writer assembly, and avoid contact with open vents, plugs, or connectors.

### **WARNING:**

**ACCIDENTAL SPILLS:** If liquids have entered the system, take it out of service and have it checked by a service technician before using it again.

To avoid electric shock or device malfunction, do not allow liquids to enter the system.

### **CAUTION:**

**DATA LOSS OR SYSTEM FAILURE:** Data loss or system failure can result due to ingress of liquids. The system does not provide protection against ingress of liquids.

Ensure installation in a cool, dry environment.

- Do not use organic solvents, ammonia-based solutions, or abrasive cleaning agents that may damage equipment surfaces.

**WARNING:**

EXPLOSION HAZARD: Flammable anesthetic vapors or liquids can cause explosions.

Do NOT use in the presence of flammable anesthetic vapors or liquids.

- Do not use metal articles, such as a screwdriver, to clean the tape heads.
- Do not bring any magnetic material near the head assembly.

**CAUTION:**

EQUIPMENT DAMAGE/DATA LOSS OR CORRUPTION/PERSONAL INJURY: This equipment contains no user-serviceable parts. Using non-approved service equipment or procedures can cause damage to the equipment, loss or corruption of data, or personal injury.

Only qualified personnel should perform the maintenance procedures.

## Visual Inspection

Perform a visual inspection regularly. Turn off the unit and remove the cover before inspecting the unit.

- Check the case and display screen for cracks or other damage.
- Inspect all cords and cables for fraying or other damage.  
Perform safety tests on any repaired line cords.
- Inspect all plugs, cables, and connectors for bent prongs or pins.
- Verify that all cords, socketed components, and connectors are securely seated.
- Verify that all keys, knobs, and power switches function properly and do not stick in one position.

If the inspection fails, do not use the unit until the failed condition is corrected.

## Check Cooling Fans and Ventilation

Use the following procedure to check cooling fans and ventilation of the units.

1. With the unit operating, verify that all fans contained in the following units are operating properly:
  - Client
  - Server
2. Check the position of the unit to ensure adequate ventilation:
  - Verify the server is in a position where the ventilation holes in the front and rear are not blocked or restricted.
  - Verify that the server is not placed near ducts, pipes, or equipment that generate heat.

**CAUTION:**

DAMAGE TO SYSTEM COMPONENTS: Poor ventilation can cause overheating.

Position the unit to ensure adequate ventilation.

## Exterior Cleaning

Clean the exterior surfaces once per month and more frequently if needed.

1. Turn off the unit and remove power before cleaning.
2. Dip a clean, soft cloth in a mild dish washing detergent diluted in water.
3. Wring the excess water from the cloth.  
Do not drip water or any liquid on open vents, plugs, or connectors.
4. Wipe the system surfaces with the damp cloth.
5. Dry the surfaces with a clean cloth or paper towel.

## Functional Checkout Procedures

Whenever a system is serviced, you must perform checkout procedures to comply with FDA guidelines and to ensure that the system is safe and functioning properly. The specific procedures depend on the service performed. Checkout procedures are separated into two categories:

- “Hardware FRU Repairs”
- “Non-FRU Repairs”

Follow the checkout procedure appropriate for the repair you performed.

**NOTE:**

For customer-supplied hardware, the customer is responsible for troubleshooting, FRU replacement, and checkouts, as they relate to hardware repairs on the system servers.

## Hardware FRU Repairs

Make FRU replacements following the appropriate repair procedures outlined in the manufacturer's manual for the system. For systems under the manufacturer's warranty, the OEM service representative may perform the repair.

**NOTE:**

Final functional checkout of the system is the responsibility of the GE Healthcare service representative onsite at the time of the repair.

The FRU checkout procedure for any listed FRU also applies to its internal PCBs and components.

## Required Tools

The following list identifies all standard tools that you may need to perform checkout procedures.

- Standard hand tools, including a #10 Torx Driver
- Antistatic wrist strap
- Can of compressed air
- Applicable Service and/or Operator manual, as needed. (Use OEM manuals as reference.)

After completing any repair, you need to complete the following checkout procedures:

- Visual Inspection: See “Visual Inspection” on page 72.
- Server: See “Server” on page 73.
- Client: See “Client” on page 73.

Locate the repaired FRU in the following tables to identify additional tools and checkout procedures to use:

### FRU Checkout Procedures

FRU Description	Additional Checkout Procedures	Additional Tools
Hard drive	See “Hard Drive” on page 73.	
Power supply	See “Electrical Safety Checks” on page 74.	<ul style="list-style-type: none"> <li>• Leakage tester</li> <li>• Multimeter</li> </ul>
Floppy drive	See “Floppy Drive” on page 73.	Floppy diskette
Optical drive	See “Optical Drive” on page 73.	CD or DVD
Display	See “Display” on page 73.	
Multimedia Card Reader (external)	See “Multimedia Card Reader” on page 74.	SD Card
Modem	See “Modem” on page 74.	
Disk Array Controller	See “Disk Array Controller (GE Healthcare-supplied server only)” on page 74.	
Tape Drive/Tape Drive Controller	See “Tape Drive/Tape Controller” on page 74.	Tape

## Visual Inspection

To conduct a visual inspection, do the following:

- Check the case and display screen for cracks or other damage.
- Inspect all cords and cables for fraying or other damage.  
Perform safety tests on any repaired line cords.
- Inspect all plugs, cables, and connectors for bent prongs or pins.
- Verify that all cords, socketed components, and connectors are securely seated.
- If the system box was opened, check that the interior is free of excessive dust buildup.  
If necessary, use commercially available compressed air to clean, following the manufacturer's instructions.

## Component Checkout Procedures

Use the appropriate checkout procedures (identified in the previous tables) to verify that the components are working properly after a Hardware FRU replacement or repair. For detailed instructions for performing any of the functional tasks (such as



acquiring data, selecting patients, and so forth), refer to the Operator's manual for your system.

## Server

### NOTE:

Verify that rack-mounted systems are fully seated and fastened to the rack before proceeding.

1. Restart the server.
2. Confirm that the system starts normally (that is, no unknown errors occur).
3. Confirm you can successfully log on to the MUSE application at the server.
4. Confirm that the user can successfully log on to the MUSE application from a MUSE client.
5. Confirm that a user can open the Edit List and access a patient record at a client workstation.

## Client

1. Restart the system.
2. Confirm that the system starts normally (that is, no unknown errors occur).
3. Confirm that the user can successfully log on to the MUSE application from a MUSE client.
4. Confirm that a user can open the Edit List and access a patient record at a client workstation.

## Hard Drive

On a system equipped with RAID, confirm that the replacement drive is operational, as described in the OEM service manual. On a single drive system, verify that the disaster recovery procedure restored the system and any available data.

## Display

1. Confirm that the display resolution is set to the recommended resolution.
2. Start the MUSE application and confirm it displays correctly.

## Floppy Drive

1. Insert the floppy disk into the disk drive.
2. Access the floppy disk using **MyComputer** or Windows **Explorer**.
3. Confirm that the system recognizes the floppy disk and you can view its contents.
4. Confirm that you can open files from and save files to the floppy disk.
5. Confirm you can acquire data into the MUSE application from the floppy disk.  
This is required only if the customer uses the floppy drive to acquire data.

## Optical Drive

1. Insert a CD or DVD into the optical drive.
2. Access the media using **MyComputer** or Windows **Explorer**.

3. Confirm that the system recognizes the media and you can view its contents.
4. Confirm that you can open files from the media.

### Multimedia Card Reader

1. Insert an **SD** card into the reader and access it using MYComputer or Windows Explorer.
2. Confirm that the system recognizes the card and you can view its contents.
3. Confirm that you can open files from and save files to the card.
4. Confirm that you can acquire data into the system from the card.

### Modem

1. Transmit an ECG from a cart to the modem.
2. In the MUSE application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Verify the **PID/Name** of the ECG transmitted from the cart was acquired.

### Disk Array Controller (GE Healthcare-supplied server only)

1. Confirm that the **C:** and **D:** drive partitions were created correctly.
2. Verify that the disaster recovery procedure restored the system database.

### Tape Drive/Tape Controller

1. Use **SQL Server Management Studio** to run a manual system backup.
2. Confirm the backup was successful.
3. Verify that all tapes were successfully used according to the backup schedule.
4. Replace tapes that are past their intended life span.

## Electrical Safety Checks

### CAUTION:

EQUIPMENT FAILURE/HEALTH HAZARD: Failure to implement a satisfactory maintenance schedule.

You need to perform these tests any time the AC ground is disturbed, for example when you service or replace the power supply or main system board.

These procedures verify that a properly wired outlet is furnishing power to the system.

1. Connect the appropriate leakage tester to the power outlet.
2. Ensure that the GND switch on the leakage tester is in the down (closed) position.

3. Refer to the following **Electrical Safety Checks** table for a description of the tests to perform.
4. Record the measurement values in your debrief.

**NOTE:**

The **Leakage Current Limits** given in the following table assume that your workstation is outside of the patient vicinity. If it is located within the patient vicinity, contact GE Healthcare for more information.

**Electrical Safety Checks**

Step	Safety Check	Condition	Result	Leakage Current Limits in Micro Amps (μA)	
				IEC 60950–1 <sup>4</sup>	UL 60950–1 <sup>4</sup>
A	Earth Leakage Current (UUT-ON in μA)			Type ITE	Type ITE
1	Forward Polarity	NC <sup>1</sup>	Pass/Fail	3500	3500
2	Neutral Open, Forward Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
3	Neutral Open, Reverse Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
4	Reverse Polarity	NC <sup>1</sup>	Pass/Fail	3500	3500
B	Enclosure Leakage Current (UUT-ON in μA)			Type ITE	Type ITE
1	Forward Polarity	NC <sup>1</sup>	Pass/Fail	3500	3500
2	Neutral Open, Forward Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
3	Ground Open, Forward Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
4	Ground Open, Reverse Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
5	Neutral Open, Reverse Polarity	SFC <sup>2</sup>	Pass/Fail	3500	3500
6	Reverse Polarity	NC <sup>1</sup>	Pass/Fail	3500	3500
E	Ground Continuity (UUT-ON in Ω)			Resistance in Ω	Resistance in Ω
1	AC mains power cord ground prong to exposed metal surface (that is, ground lug)	N/A <sup>3</sup>	Pass/Fail	Less than 200 mΩ	Less than 200mΩ

<sup>1</sup>NC = Normal condition

<sup>2</sup>SFC = Single Fault Condition

<sup>3</sup>N/A = Not Applicable

<sup>4</sup>Countries recognizing IEC standards use IEC values. Countries recognizing UL standards use UL values.

## Non-FRU Repairs

System functional checks are required for non-FRU repairs and typically involve system setup and configurations that you can perform remotely or onsite. If you perform them remotely, the remote support engineer can confirm them through remote access, or verify them with the customer contact. For additional instructions, refer to the Operator's manual for your system.

### Printing

Use the following procedures to verify that the printing functions are working correctly.

#### Manual Print Checkout

1. Highlight a record on the **Edit** list and click **Print**.
2. From the drop-down menu, select the printer you want to test and click **OK**.
3. Verify that the record printed out correctly at the selected printer.

#### Automatic Print Checkout

1. Acquire data from a cart/stress device with the location number you are testing.
2. Verify that the record prints out correctly at the printer set up for automatic distribution.

#### Format Setting Change Checkout

1. Highlight a record on the **Edit** list and click **Print**.
2. From the drop-down menu, select the printer you want to test and click **OK**.
3. Compare the new printout to a previous printout to verify format changes took effect.

### Faxing

Use the following procedures to verify that the faxing functions are working correctly.

#### Manual Fax to Temp or Defined Device Checkout

1. Highlight a record on the **Edit** list and click **Print**.
2. Send the record to a temporary fax machine.
3. Check that the fax printed correctly at the receiving fax machine.

#### Automatic Fax to Existing Fax Device Checkout

1. Acquire data from an ECG cart with the location set up for the correct report distribution, or confirm data with correct physician mapping for auto-fax.
2. Check that the fax printed correctly at the receiving fax machine.

### Editing/Confirming

Use the following procedures to verify that the editing and confirming functions are working correctly.

#### Edit Record Checkout

1. Have the customer open a record on the **Edit** list.
2. Update the record in the **Edit** list.
3. Re-open the record to verify the changes were saved.

### Confirm Record Checkout

1. Have the customer open a record on the **Edit** list.
2. Have the customer confirm the record.
3. Do a retrieval of the record and verify that it is now in the database.

### Report Distribution Checkout

Use the following procedures to verify that the report distribution function is working correctly.

1. Acquire or confirm data for the location of a new report distribution setup.
2. Check the output device setup in the report distribution for the report.

### Device Setup

Use the following procedures to verify that the devices are set up correctly.

#### Output Device (Printer, Fax, HL7 Results)

1. Highlight a record on the **Edit** list and click **Print**.
2. From the drop-down menu, select the newly created device and click **OK**.
3. Check the device for the report.

#### Inbound Device (Modem, Share)

1. Transmit a record from a source device.
2. Verify that the record is displayed in the application.

### User Setup

Use the following procedures to verify that the user is set up correctly.

1. Have a newly created user start the application.
2. Have the user log on and confirm application access based on roles/privileges given during setup.

### Carts Transmission/Acquisition

Use the following procedures to verify that the Carts transmissions and acquisitions functions are working correctly.

#### Modem Transmission Checkout

1. Transmit an ECG from the cart to a modem.
2. In the application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

#### Wireless Transmission Checkout

1. Transmit an ECG from a cart while in range of a wireless antennae.
2. In the application, select **System Status**.

3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

#### LAN Transmission Checkout

1. Transmit an ECG from a cart through the LAN.
2. In the application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

#### Removable Media Acquisition

1. Insert the media into the client.
2. Acquire the media through **MUSE Acquisition**.
3. In the application, select **System Status**.
4. Select **Newly Acquired** or **Acquisition Log**.
5. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

### MARS Transmission

#### MARS to MUSE Setup Checkout

1. From a MARS workstation, send a Holter report to the MUSE system.
2. In the application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the PID/Name of the ECG transmitted from the MARS system was acquired in the MUSE system.

#### MARS Formatted Report Print Checkout

1. In the MUSE system, highlight a Holter report on the **Edit** list or retrieve a record from the database.
2. Click **Print**.
3. Compare the newly printed Holter report to the printout prior to the MARS formatter installation and check that the Holter format changed.

### CASE/Cardiosoft Transmission

1. Send a **Stress** report to the MUSE system.
2. In the application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

## Monitoring Transmission

Manual transmission from a bedside monitor

1. From the **Bedside/Dash** monitor, transmit 12SL to the MUSE system.
2. In the MUSE system, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Check that the **PID/Name** of the ECG transmitted from the cart was acquired in the application.

## Database Search

Use the following procedures to verify that the database search function is working correctly.

### Manual Search Checkout

1. Go to the **Database Search** function of the application.
2. Create a search.
3. Choose criteria and run the search.
4. Verify that the search results match the selected criteria.

### Automatic Search Checkout

1. Go to the **Database Search** function of the application.
2. Create a search.
3. Save the criteria.
4. Schedule the search.
5. Verify that the search runs when scheduled and expected results are generated.

The MUSE v8 system runs all scheduled searches only once per day.

## Web Retrieval Checkout

Use the following procedures to verify that the retrieval checkout functions are working correctly.

### MUSE Web Data Retrieval Checkout

1. Start **Internet Explorer**.
2. In the **URL** field, type the MUSE server name (for example, **http://museserver**).  
If prompted, log in as a user who has access to MUSE Web.
3. Choose **Frames** or **No Frames**.
4. In the **PID** field, type the patient ID, or in the **Last Name** field, type the patient name.
5. Find the record to verify that MUSE Web is working properly.

### CV Web Data Retrieval Checkout

1. Start **Internet Explorer**.
2. In the **URL** field, type the CV Web server name (for example, **http://cvweb**).  
If prompted, log in as a user who has access to MUSE Web.

3. In the **PID** field, type the patient ID, or in the **Last Name** field, type the patient name.
4. Verify that the appropriate MUSE server/site is selected.
5. Find the record to verify that CV Web is working properly.

## Remote Support

Use the following procedures to verify that you can access the system for remote support.

1. Log on to the customer's system using the remote connection configured for that system (pcAnywhere or InSite ExC).
2. Confirm that you can access the customer's desktop via the remote connection.
3. Confirm that you can upload and download files to the customer's system.

## HIS/CCG

Use the following procedures to verify that the HIS and CCG functions are working correctly.

### HIS ADT/Orders Inbound Checkout

1. From the MUSE system, go to the **HIS Event Viewer**.
2. Verify that **Inbound ADT** and **Order** events exist.
3. Have the customer verify that the MUSE system is receiving the data they are sending from their interface.

### HIS Realtime Results/Billing Outbound Checkout

1. From the MUSE system, go to the **HIS Event Viewer**.
2. Verify that **Outbound Results/Billing** events exist.
3. Verify that outbound data is leaving the MUSE results/billing queue.

### HIS Batch Billing

1. From the MUSE system, go to **System > Status**.
2. View the **HL7 Batch Log** and verify that the **Batch** was sent and it succeeded.

### Order Download from MAC Cart Checkout

1. From a MAC cart, use the **Order Download** function.
2. Verify that the MAC cart is able to successfully download the order from the MUSE system.

## XML Import

Use the following procedures to verify that import XML data correctly.

1. Copy XML data files from the manufacturer's device into the XML folder set up on the MUSE server.
2. In the application, select **System Status**.
3. Select **Newly Acquired** or **Acquisition Log**.
4. Verify that the XML data was acquired into the MUSE system.



## Backup

Use the following procedures to verify that the backup procedures work correctly.

1. Use **SQL Server Management Studio** to run a manual MUSE backup.
2. Confirm that the backup was successful.

## Login

Use the following procedures to verify that the MUSE and Windows Authentication procedures work correctly.

### MUSE Authentication

1. Have the user log on to the MUSE system using MUSE Authentication.
2. Verify the user is able to successfully log on to the MUSE system.

### Windows Authentication

1. Have the user log on to the MUSE system using Windows Authentication.
2. Verify the user is able to successfully log on to the MUSE system.

### Via Citrix Using MUSE Authentication

1. Have the user log on to the MUSE system using MUSE Authentication.
2. Verify the user is able to successfully log on to the MUSE system.

### Via Citrix Using Windows Authentication

1. Have the user log on to the MUSE system using Windows Authentication.
2. Verify the user is able to successfully log on to the MUSE system.

## Discarding/Recovering/Deleting Data

Use the following procedures to verify that the user can discard, recover and delete a test.

### Discarding Data

1. Have the user discard a test from a MUSE site database.
2. Verify the test was successfully discarded and is displayed on the **Discarded Data List** and as a log entry on the **Discard Log**.

### Recovering Data

1. Have the user recover a test from the **Discarded Data List**.
2. Verify that the test was successfully recovered and is displayed on the appropriate MUSE site database and as a log entry on the **Discard Log**.

### Deleting Data

1. Have the user delete a test from the **Discarded Data List**.
2. Verify the test was successfully deleted from the system and is displayed as a log entry on the **Discard Log**.



# 6

## HL7 System State Backup and Recovery

A backup and recovery plan for the HL7 server is crucial to ensure that you can recover the HL7 configuration should the server fail or files become corrupted.

Coordinate recovery of the HL7 System State with the GE Healthcare HL7 engineer.

### Copying the System State Backup

After installation and testing of the HL7 interface is complete, the GE Healthcare HL7 engineer creates a weekly backup job that saves the HL7 configuration in the **C:\Systemstate** folder on the HL7 server. It is the customer's responsibility to copy this folder to a network drive or external media to ensure that you can restore the HL7 configurations if you need to fully rebuild the server. A local copy of the folder should remain on the server.

### Disaster Recovery

There are several reasons why you might need to perform a disaster recovery. This procedure describes a situation where you need to rebuild the server and return it to its original manufactured state. Using this recovery method deletes all information on the system's hard drive.

Before performing a full disaster recovery, consider other methods available to recover the system, such as starting in Safe Mode, rolling back newly installed drivers, using the Last Known Good Configuration option, and other conventional Windows restore options. For more information, refer to the Microsoft Web site.

### Before You Begin

Check if a copy of the **SystemState** folder exists on the network or external media. This folder is created once a week and contains a backup of the HL7 configuration. If an external copy does not exist and you are still able to log on to the server, make a copy of the **SystemState** file located in the **C:\gehc-it\backup\data** folder before starting the disaster recovery process.

If you are able to log on to the server, save the InSite ExC configuration as described in the **InSite ExC Installation and Configuration Guide**.

# Rebuilding the HP DL360 G5 Server

## Configuring the Server

This procedure is only for the GE Healthcare-supplied HP DL360 G5 server. It restores the system to its original manufactured state.

Verify that you have the following software CDs:

- 2003801-012 HP SmartStart CD v7.60
- 2030821-001 MUSE HIS HP#325367-004
- 2038348-001 MUSE Win 2003 Server SP2

1. Start the system using the **SmartStartCD v7.60**.  
This takes approximately three minutes.
2. Press **F1** to continue, if applicable.
3. At the **Language selection** window, select the **English** option.
4. On the **Select the keyboard to be used with the system** drop-down list, select **English** and click **Continue**.
5. Click **Agree** to accept the License Agreement.
6. Select **Maintain Server**.
7. Select **Erase System**.
8. Confirm all boxes are selected and click **Continue**.
9. When the **Are you sure...?** window opens, click **OK**.  
The system powers down and then restarts. (This takes approximately three minutes.)
10. During startup, when prompted, press **F9** for the **ROM-based Setup Utility**.
11. Select **Boot Controller Order** and move **PCI slot 1 HP Smart Array Controller** to the top of the list.  
The controller is identified as **E200i**.
12. Press **Enter**.  
**NOTE:**  
If necessary, press **Esc** to return to the **Selection** menu.
13. Select **Date and Time** and press **Enter**.
14. Enter the current date and time and press **Enter**.
15. Select **Server Availability** and press **Enter**.
16. Select **POST F1 Prompt** and press **Enter**.
17. Select **Disabled** and press **Enter**.
18. Press **Esc** to exit the window.
19. Press **Esc** to exit the utility.
20. Press **F10** to **Confirm Exit Utility**.

## Configuring the RAID

1. Restart the system with HP **SmartStartCD v7.60** in the optical drive.
2. At the **Language selection** window, select the **English** option and click **Continue**.
3. In the **Select the keyboard to be used with system** drop-down list, select **English** and click **Continue**.
4. Select the **Agree** option to accept the License Agreement and click **OK**.
5. Click **Maintain Server** to begin configuration of the array controllers.
6. Click **Configure Array**.
7. Under **Common Tasks**, select **Clear Configurations**.
8. Select the **Select All** check box and click **OK**.
9. Select **Create Logical Drive**.  
The **Create Logical Drive** window opens.
10. Click **OK** to use the default settings.
11. In the **Configuration View** panel, confirm the SCSI controller has one logical drive configured to **RAID 1+0**.
12. Click **Exit ACU**.
13. Click **Smartstart Home...**
14. Click **Deploy Server**.
15. Click **Continue**.
16. Click the **Microsoft Windows** folder.
17. Select **Microsoft Windows Server 2003, Standard Edition (HP-branded)**, and click **Continue**.
18. In the **Operating system media source**, select the **CD-ROM** and **Flat Files** options, and click **Continue**.

**NOTE:**

It takes several minutes while SmartStart prepares the system for installation of the operating system.

19. In the **File System** drop-down box, select **NTFS**.
20. Under the section **Select Boot Partition Size**, verify that **Maximum** is selected, and click **Continue**.
21. In the **User Name** field, type <Hospital Name>.
22. In the **Organization** field, type <Hospital Name>.
23. In the **License Type** field, select **Per Seat** and click **Continue**.
24. On the **SNMP Configuration** window, accept the default entries and click **Continue**.

**NOTE:**

It takes several minutes while **SmartStart** prepares the system for installation of the operating system.

When the **SmartStart CD** ejects from the optical drive and you are prompted to insert the operating system media, proceed with ["Installing Windows Server 2003"](#).

## Installing Windows Server 2003

1. On the **Please insert the Operating System media and click Continue** window, remove the **SmartStartCD** and insert the **Windows 2003 Server CD (GE PN 2030821-001; HP PN 325367-004)** and click **Continue**.

The system restarts after three to five minutes.

2. When the CD drawer opens, remove the **Windows 2003 Server CD**.

The system restarts several times over three to five minutes.

3. When the **Welcome to Windows Setup Wizard** window opens, click **Next**.

The **Installing Devices** window opens for several minutes.

4. On the **Regional and Language Options** window, click **Next**.

5. On the **Computer Name and Administrator Password** window, follow the screen instructions and use the following information where applicable. Case sensitive inputs are required.

Field	Values
<b>Computer Name</b>	Revise per customer or accept the default
<b>Administrator Account Password</b>	Enter the GE Healthcare-recommended Administrator password, or enter the customer-provided Administrator password.
<b>Confirm Password</b>	Enter same password entered in the previous field.

6. Click **Next**.
7. Set the **Date & Time** and **Time Zone** to appropriate values and click **Next**.  
The system displays **Installing Network** for 30 seconds.
8. Select No, this computer... or Yes, make this computer... per the customers' network environment.
9. In the text box, type **HIS\_WG**, or enter the domain or workgroup name per the customer order and click **Next**.  
The system installs drivers and programs for approximately 20 minutes and then restarts.
10. On the **Welcome to Windows** window, press **CTRL+ALT+DEL** and enter the password.
11. On the **Windows Server Post-Setup Security Updates** window, click **Finish**.
12. On the **When you close this page...** window, select **Yes**.
13. On the **Manage Your Server** window, select the **Don't display this page at logon** check box.
14. Exit the **Manage your server** window.

## Configuring Display Settings

1. Click **Start > Control Panel > Display**.
2. Click on the **Settings** tab and configure the **Settings** in **Display Properties** as follows:
  - a. Set the **Screen Resolution** to **1024 x 768 pixels**.
  - b. Set the **Color Palette** to **Highest 32 bit**.
  - c. Click **Advanced** and select the **Monitor** tab.
  - d. Set the **Screen refresh rate** to **75 Hertz** and click **OK**.
  - e. Click **Apply**.
  - f. On the **Testing Mode** dialog box, click **Yes**.
  - g. Click **OK** to exit the **Display Properties** window.

## Setting Up the Windows Environment

1. From the **Control Panel**, click the **System** icon.  
The **System Properties** window opens.
2. Click the **Advanced** tab.
3. Click **Startup and Recovery Settings**.
4. In the **Time to display list of operating systems** text box, enter **5** seconds.
5. in the **Write debugging information** drop-down box, select **(none)**.
6. Click **OK** to exit the **Startup and Recovery** window.
7. Click **OK** to exit the **System Properties** window.

## Installing Windows 2003 Service pack 2

1. Insert the **Win 2003 Server SP2 CD** into the server optical drive.  
This CD ships with the **MUSE v8 Core Software Kit**.
2. Click the **Windowsserver2003-KB914961-SP2-x86-enu.exe** file.  
The **Service Pack 2** files are extracted and the **Windows 2003 Service Pack 2** installer opens.
3. Follow the prompts to install the Service Pack.
4. Restart the server after installation is complete.

After completing the rebuild process go to ["Verify Help and Support Service "](#) on [page 90](#).

## Rebuilding the HP DL360 G7 Server

This procedure is only for the GE Healthcare-supplied HP DL360 G7 server. It restores the system to its original manufactured state.

Verify that you have the following software:

2062765-019 DVD IMAGE DL360G7 CCG SERVER 2003

**NOTE:**

Before starting, disconnect the mouse from the USB port. This connection can cause problems when selecting the function keys using the keyboard during the rebuild process.

## Verify the Boot Sequence

1. Restart the server
2. During the restart, when prompted to **Press any key to view Option ROM messages** press **F9 Setup**.  
The **ROM-based Setup Utility** opens.
3. Select **Standard Boot Order (IPL)** and press **Enter**.  
The **Standard Boot Order (IPL)** window opens.
4. Verify that **CD-ROM** is listed as the first boot sequence. This is necessary to ensure that the system can start from the MUSE Image CD. If the boot sequence is correct skip this section and go to [“RAID Configuration” on page 88](#). If **CD-ROM** is not listed as the first boot sequence, do the following:
  - a. Use the arrow keys to select **CD-ROM** and press **Enter**.
  - b. Select **Set the IPI Device Boot Order** to **1** and press **Enter**.  
The **CD-ROM** moves to the first position in the boot sequence.
  - c. Press **Esc** twice to close the menu and the **ROM-based Setup Utility**.
  - d. Press **F10** to confirm.  
The system will reboot.

## RAID Configuration

1. Power on the server.
2. Allow the server to proceed through the **Power and Thermal Calibration in Progress** screen.
3. When prompted, press any key to view **Option ROM** messages.
4. When prompted, press **F8** to run the **Option ROM Configuration For Arrays Utility**.
5. Select **Delete Logical Drive** and press **Enter** to proceed.
  - a. If there are no logical drives available, proceed to step 6.
  - b. Press **F8** to delete the logical drive.
  - c. Press **F3** to confirm the deletion of the logical drive.
  - d. Press **Enter** to continue.
6. Select **Create Logical Drive** and press **Enter** to proceed.  
The **Array Configuration** screen opens, select the following:
  - a. **Available Physical Drives:** Both drives selected
  - b. **RAID Configurations:** **RAID 1+0**
  - c. **Parity Group Count:** None selected



- d. **Spare:** None selected
- e. **Maximum Boot partition:** *Disable (4GB maximum)*
7. Press **Enter** to create a logical drive.
8. Review the configuration and press **F8** to save the configuration.
9. Press **Enter** to continue.
10. Select **View Logical Drive** and press **Enter**.
11. Verify that the new logical drive has been created with the following settings:  
**Logical Drive #1, RAID 1+0, 600.09 GB**
12. Press **ESC** to return to the Main Menu.
13. Press **Esc** to exit the utility.
14. If the mouse was disconnected earlier in the process, reconnect it now.

## Applying the Server Image

The image will:

- Install Windows 2003 Server R2 Standard edition
- Install Windows 2003 Service Pack 2
- Set screen resolution to 1280 x 1024 pixels
- Assign a password to the built-in administrator account

To image the server use the following steps:

1. Power on the server.
2. Immediately place *2062765-019 DVD IMAGE DL360G7 CCG SERVER 2003* into the DVD-ROM drive of the server.
3. Allow the server to boot the image DVD.
4. Allow the imaging utility to start.
5. When prompted to continue image the drive, press **Y**.
6. The **Ghost utility** will apply the image to the server hard drives.
7. Allow the imaging process to finish and verify that the image has been applied successfully.
8. Once the image has been applied and verified, a **Success** message will be displayed.
9. Remove the image DVD and restart the server.
10. Allow the server to boot until the **Windows Setup Wizard** opens.
11. On the **Welcome to the Windows Setup Wizard** screen do the following:
  - a. Click **Next**.  
The **License Agreement** screen opens.
  - b. Select **I accept this agreement**.
  - c. Click **Next**.

12. On **Date and Time Settings** screen set the following:
  - a. **Date**
  - b. **Time**
  - c. **Time Zone**
  - d. **Automatically adjust clock to daylight savings changes**
13. Click **Next**.
14. Windows will finish the configuration and reboot the server.
15. Verify you can log on the operating system using the built-in administrators account, If you do not remember the administrator password contact GE Healthcare Technical Support.

Proceed to ["Verify Help and Support Service "](#) on page 90.

## Verify Help and Support Service

Microsoft reported cases of **Help and Support** not running after Windows 2003 SP2 was installed. Verify, and if necessary, install **Help and Support** as follows.

1. Select **Start > Help and support**.
2. If the following message is displayed go to step 3. If **Help and Support** opens ignore this section and proceed to ["Configuring SNMP" on page 90](#).  
  
**Windows cannot open Help and Support because a system service is not running.**
3. To fix this problem, start the service named **Help and Support** by opening a command prompt
  - a. Type `cd \Windows\PCHealth\HelpCtr\Binaries`
  - b. Type command: `start /w helpsvc /svchost netsvcs /regserver /install`
  - c. When the command completes, the **Services** should display the **Help and Support** service.
4. Start the **Help and Support** service.

Proceed to ["Configuring SNMP" on page 90](#).

## Configuring SNMP

**SNMP** is enabled by default. Some customers may want it disabled in order to reduce security risks in the system. To disable **SNMP** use the following steps.

1. Select **Start > All Programs > Administrative Tools > Services**.
2. In the right pane, open **SNMP Service**.
3. Select the **General** tab.
4. At **Startup type**, click **Disabled**.
5. At **Service status**, click **Stop**, if it is not grayed out.
6. On the **Stop Other Services** window, click **Yes**.

7. After the **Stopping Services** window closes, click **OK** to close the **SNMP Service Properties** window.
8. Close the **Services** window.

After the server has been restored, complete the recovery process by *Installing CCG*, *Installing InSite ExC*, and *Restoring the System State* as described in the next sections.

## Installing CCG

Follow the instructions in the **MUSE Cardiology Information System Installation Manual** to install and verify CCG on the server.

## Installing InSite ExC

Install InSite ExC on the server using the **InSite ExC Installation and Configuration Guide**. Configure it using the same serial number that was originally used to register the server with the back office. If you were able to save the InSite configuration before rebuilding the server, you can use the **InSite Restore Configuration** function to restore the original configuration values.

## Restoring System State

After the server is restarted, contact the GE Healthcare HL7 engineer to restore the HL7 configuration from the System State backup.



# MUSE System Backup and Recovery

## Introduction

A backup and recovery plan is crucial to prevent data loss and to minimize service interruption in the event of system failure or disaster. This chapter describes the backup and recovery options provided by GE Healthcare. These options are available only to users running the MUSE system on GE-supplied hardware. Users running the software-only version of the MUSE system, or who choose not to use the GE-supplied options, are responsible for implementing and maintaining their own backup and recovery plans.

GE Healthcare provides two backup options.

- A network backup option is available for users running MUSE system on GE-supplied G5 or G6 platforms.
  - A tape backup option is available for users running the MUSE system on GE-supplied G4 or G5 platforms equipped with the AIT Tape Drive.
- Refer to [“Backup Options” on page 94](#) for more information.

After determining which backup option you will use, refer to [“Setting Up Automatic Backups” on page 97](#) for instructions on how to create the backup jobs, how to configure the backup jobs, how to change the backup schedules, how to create automatic notifications, and how to test the backup jobs.

In addition to running automatic backup jobs at regularly scheduled times, you can manually initiate the backup jobs to run outside of their normal schedules. Use this feature if you need to generate a special backup, for example, before upgrading or performing service on the system. Refer to [“Backing Up the Database Manually” on page 109](#) for more information.

In the event that the database becomes corrupted, or if you want to return the database to a previous state for any reason, you can restore just the MUSE database. For details, refer to [“Database Recovery” on page 109](#).

**NOTE:**

In the event of a system-wide failure or natural disaster, or if you want to return the system to a previous state for any reason, you can restore the entire MUSE system. For details, refer to [Appendix A “System Recovery” on page 117](#).

During the backup and recovery process, it may be necessary to shut down or restart the MUSE system or to initialize a new backup tape. For details, refer to [“Additional Information” on page 115](#).

# Backup Options

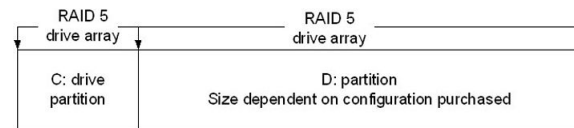
This section provides the following information about the MUSE backup options:

- Overview of the MUSE disk and data structures.
- Overview of the network and tape backup options.

## Overview of the MUSE Disk and Data Structures

Knowledge of the MUSE disk and data structures helps you understand the backup options provided by GE Healthcare. If you purchased a software-only system, or if you choose not to use the GE-supplied backup options, this information is useful in planning and implementing your own backup/recovery plan.

MUSE servers running on GE-supplied hardware are configured with two partitions, as shown in the following diagram:



The **C:** drive is fairly static and typically needs to be backed up only for operating system updates, software upgrades, or configuration changes. It contains the following components:

- The Windows operating system
- SQL Server software - including the master and **msdb** system databases
- The MUSE client application
- GE Remote Access Files (InSite ExC)

The **D:** drive is dynamic and typically needs to be backed up on a regular basis. It contains the following components:

- The MUSE user databases (**d:\muse\db**)
- The backup report and supporting files (**d:\muse\backup\**)
- The temporary files being sent to the MARS formatter when Holter reports are printed (**d:\muse\mars**).
- The XML input files (**d:\muse\xml**).
- The acquisition data sent through a network share (**d:\muse\acq**).

The MUSE system, version 7.0.2 and above, uses the SQL Server 2005 Database Management System (DBMS) and includes the following default user databases:

- **MUSE\_Site0001**
- **MUSE\_SiteTemplate**
- **MUSE\_System**

If additional sites have been set up on the system, additional site databases will exist; for example, **MUSE\_Site0002**, **MUSE\_Site0003**, and so on.

## Overview of the Network and Tape Backup Options

For customers running on GE Healthcare-supplied hardware, GE Healthcare provides a network option and a tape option for backing up the MUSE system and databases. Your hardware platform determines which options are available, as shown in the following table.

Platform	Tape Backup	Network Backup
HP ML370 G4	x	
HP ML370 G5	x	x
HP DL370 G6		x

### CAUTION:

**LOSS OF DATA/DATA CORRUPTION:** The backup procedures in this chapter were tested only on the GE-supplied hardware outlined in the previous table. GE Healthcare cannot guarantee database or system recovery following these procedures on customer-supplied hardware.

Customers implementing the network backup model described in this document on their own hardware are responsible for testing, verifying, and maintaining the procedure.

GE Service supports both the tape and network backup options, as covered by any applicable warranties or service agreements. GE Healthcare Service also assists with the initial setup and configuration of the selected option.

The MUSE backup options are set for the Simple Recovery Model. Customers who require a Full Recovery Model (so that they have transaction logs that provide the ability to recover to a specific point in time) need to implement their own backup and recovery plans. Customer-implemented backup plans are not covered by applicable warranties or service agreements; however, GE Healthcare Service can still assist in these cases on a time-and-material basis.

### NOTE:

Even though GE Healthcare Service may install and configure the backup options, the customer is responsible for verifying that each backup completed successfully. You cannot use the success or failure status of the SQL backup job itself as proof of the job's success; in some circumstances, the SQL job can indicate a false success.

You have two methods for verifying the success of a backup job:

- Review the backup log file generated at the completion of each backup. The log file can be emailed to a selected user for review. Refer to [“Creating Notifications” on page 103](#) for details.
- Verify the database backup files and their dates. Refer to [“Network Backup Option” on page 95](#) for a list of the backup files created on the network drive.

## Network Backup Option

The network backup option is available to users running MUSE v7.1.1 or higher on GE Healthcare-supplied G5 or G6 platforms. It provides both nightly and weekly backup jobs.

## Nightly Backup

The nightly backup job, **7Nightly\_Backups**, does the following:

- **Creates a daily backup file for each database.**  
The files are named by combining the day of the week with the name of the database, as seen in the following examples:

- MondayMaster.bak
- Mondaymsdb.bak
- MondayMUSE\_Site0001.bak
- MondaySiteTemplate.bak
- MondaySystem.bak

This results in seven sets of backup files. Each file overwrites the corresponding file from the previous week.

- **Performs a full backup of all the MUSE databases.**  
The advantage of a full backup is that you can restore the databases using a single backup instead of a series of differential or incremental backups. The disadvantage of a full backup is that it requires more storage space than a differential or incremental backup. Because the backup job creates seven sets of backups (one for each day of the week), the destination drive for the backups must be at least seven times greater than the combined size of the databases. For example, if the MUSE databases totalled 20 GB, the destination drive would need to be at least 140 GB (7 x 20 GB) to hold a full seven-day backup cycle.
- **Saves the backup to a local folder and then copies it to a network share.**  
You can edit the script file, **7Nightly\_Backups\_NetCopyScript.bat**, to customize this behavior in two ways:
  - First, you can modify the way in which the backup files are copied to the network drive by setting the **COPYOPTION** parameter to one of the following values:
    - **MIRROR** - Copies the nightly database backups from the local drive to the network share, leaving the originals on the local drive. This provides a full set of backups on both the local drive and the network share.
    - **MIRRORSOME** - Copies a defined number of backup sets from the local drive to the network share, leaving the defined number of originals on the local drive and removing the remainder. This provides a partial set of backups on the local drive and a full set of backups on the network share.  
To define the number of records to retain on the local drive, set the **LOCALDAYSTOMAINAIN** parameter with a number from 1 to 7. For example, setting **LOCALDAYSTOMAINAIN=3** retains the three most recent nightly backups on the local drive.
    - **MOVE** - Copies the nightly database backups from the local drive to the network share and removes the originals from the local drive. This provides only one set of backups on the network share.
  - Second, you can change the location of the network share where the backups will be copied.
- **Attempts to reconnect if the network connection is interrupted.**  
The backup job uses the **robocopy** command to copy or move the backup files from the local directory to the network share. If the network connection is interrupted during the transfer, **robocopy** notes where the copy stopped, attempts to reconnect to the network, and resumes the transfer.



## Weekly Backup

The weekly backup job, **WeeklyCDriveNetworkBackup**, backs up the complete **C:** drive, including the system state, to a shared network drive. The weekly backup job saves the files directly to the network drive; unlike the nightly backup job, it does not first save the files locally and then copy them to the network drive.

By default, the weekly backup job saves the backup file, **CDrivebackup.bkf**, to the local **d:\muse\backup** folder. To change the destination to a network share, edit the location in the weekly backup batch file, **Cbackup\_NO\_TAPE.bat**. For instructions, refer to [“Configuring the Backup Jobs” on page 99](#). The backup file is overwritten each time the weekly backup runs.

Unlike the weekly tape backup (see [“Local Tape Backup Option” on page 97](#)), the weekly network backup is not intended for use as part of an Automated System Recovery (ASR). Instead, when using the weekly network backup, recovery involves the using the server image CD and weekly backup file. For details, refer to [Appendix A “System Recovery” on page 117](#).

## Local Tape Backup Option

The local tape backup option is available only on GE Healthcare-supplied G4 servers, for which a tape drive was supplied as standard equipment, and G5 servers, for which a tape drive was available as optional equipment. The tape drive is no longer available for purchase. Any G5 server that does not already have a tape drive must use the network backup option [“Network Backup Option” on page 95](#).

The local tape backup option includes nine AIT tapes and provides a nightly backup, a weekly backup, and a monthly backup.

### Nightly Backup

The nightly backup copies each of the MUSE user databases to an AIT tape. This backup job requires seven of the nine AIT tapes, each labeled with a day of the week from **Sunday Backup** through **Saturday Backup**.

### Weekly Backup

The weekly backup copies the entire **C:** drive to an AIT tape. This backup job requires one of the nine AIT tapes, labeled **Weekly C: Backup**.

### Monthly Backup

The monthly backup copies the entire MUSE system to an AIT tape. This backup job requires one of the nine AIT tapes, labeled **Monthly System Backup**.

# Setting Up Automatic Backups

This section provides the following information for creating and configuring automatic backups:

- Creating the backup jobs
- Configuring the backup jobs
- Changing the backup schedules
- Creating notifications
- Testing the backup jobs

## Creating Backup Jobs

The procedure for installing the network backup jobs and the procedure for installing the tape backup jobs are nearly identical. The only difference between them is the name and location of the files to install. That difference is noted where applicable.

### NOTE:

If you are creating backup jobs on an existing system, do the following before proceeding:

- Delete any backup files located in the **d:\muse\backup** folder.
- Delete any SQL backup jobs in **SQL Server Management Studio**.

To create the backup jobs, do the following:

1. Create the **d:\muse\backup** folder if it does not already exist.
2. Insert the MUSE support CD into the optical drive.
3. Copy all the files from **\Local Tape Backup** on the support CD to **d:\muse\backup** on the MUSE server.

The SQL backup jobs utilize batch files stored in the **d:\muse\backup** folder. If the backup folder is created on a different drive partition, or uses a different name, the backup jobs and email notifications will fail.

4. Verify that the **SQL Server Agent** service is running using the **MUSEBkgnd** account.

The **SQL Server Agent** service runs SQL jobs, such as the backup jobs. It is also required for database searches and the log and queue maintenance jobs. Use the following procedure to verify the service is running:

- a. Select **Start > Administrative Tools > Services** to display the **Services** list.
  - b. Right-click **SQL Server Agent** and select **Properties**.
  - c. Verify that the **startup type** is set to **Automatic** and change it if necessary.
  - d. Start the **SQL Server Agent** service if it is not already running.
  - e. Close the **Services** window.
5. Do one of the following to build the appropriate backup jobs:
    - **To build the network backup jobs:**
      - a. Open a **Command Prompt** window.
      - b. Run **d:\muse\backup\build\_7Day\_job.bat**.  
This creates the following backup jobs and schedules

Job Name§	Scheduled Run Time§
7Nightly_Backups§	Daily starting at midnight §
WeeklyCDriveNetworkBackup§	Every Friday starting at 3:00 PM§

You receive the message **Warning: Non-existent step referenced by @on\_fail\_step\_id**. This warning is normal and you can ignore it.

- c. In the **SQL Server Management Studio**, expand **SQL Server Agent > Jobs** and verify the two backup jobs were created.

- **To build the local tape backup jobs:**

- a. Open a **Command Prompt** window.
- b. Run **d:\muse\backup\buildjobs.bat**.  
This creates the following backup jobs and schedules:

Job Name§	Scheduled Run Time§
NightlyMUSEDDBBackup§	Daily at 2:00 a.m.§
MonthlyMUSEDDBBackup§	First Monday of the Month at 9:00 a.m.§
WeeklyCDBBackup§	Each Friday at 3:00 p.m.§
NightlyBackupReminder§	Daily at 3:00 p.m.§
MonthlyBackupReminder§	First Monday of the Month at 6:00 a.m.§
WeeklyBackupReminder§	Each Friday at 1:00 p.m.§

It also adds a backup device under **Server Objects > Backup Devices**. If the device already exists, you receive an error message that the device already exists. You can ignore this error.

- c. In the **SQL Server Management Studio**, expand **SQL Server Agent > Jobs** and verify the backup jobs were created.

**NOTE:**

If the backup jobs already exist, the batch files do not overwrite them. This prevents you from accidentally removing any custom configurations. To replace the existing jobs with the defaults, run **SQL Server Management Studio**, open **SQL Server Agent > Jobs**, and delete the existing jobs before you run the batch files.

## Configuring the Backup Jobs

After the backup jobs are installed ([“Setting Up Automatic Backups” on page 97](#)), configure them to run at a time and in a manner that meets your operational needs.

## Configuring the Network Backup Jobs

Before configuring the network backup jobs, gather the following information:

- The **COPYOPTION** parameter to use.  
Refer to [“Nightly Backup” on page 96](#) for details.
- The sizes of the MUSE database and **C:** drive.

The size of the MUSE database and **C:** drive determine the required amount of free space on the destination drive. For example:

Target	Size	Number	Space Needed
MUSE Databases	20 GB	7	140 GB
C: Drive	10 GB	1	10 GB
Space needed on the destination drive			150 GB

Allow additional space to accommodate anticipated growth.

#### NOTE:

Because the backup procedure first backs up to the local drive and then moves the backed up files to the network share, the local drive needs enough free space to accommodate at least one backup. For example, if the MUSE databases total 20 GB, the local drive must have at least 20 GB of free space or the backup fails.

- The location of the destination network share.  
You need this information to edit the **7Nightly\_Backups\_NetCopyScript.bat** and **Cbackup\_NO\_TAPE.bat** files. The path to the network share cannot contain spaces; if it contains spaces, the backup fails.

#### NOTE:

After you have identified the location of the destination network share, do the following:

- Create a folder called **MUSEbackups** on the share drive.
- Share it on the network.
- Grant **Full Control** to the **MUSEBkgnd** account.  
This should be the same account as the **SQL Server Agent** service account logon on the MUSE server.

### Configuring the Nightly Network Backup

- Create the folder **d:\muse\musedbbackups**.
- Using an ASCII editor such as Notepad, open **d:\MUSE\Backup\7Nightly\_Backups\_NetCopyScript.bat**.
- Set **COPYOPTION** to **MIRROR**, **MIRRORSOME**, or **MOVE**.  
For example: **SET COPYOPTION=MOVE** Refer to "Nightly Backup" on page 96 for details.
- If you set the **COPYOPTION** to **MIRRORSOME**, set the **LOCALDAYSTOMAINAIN** parameter to the number of backups to keep on the local drive.  
For example: **SET LOCALDAYSTOMAINAIN=3** retains the three most recent backups on the local drive.
- Set the **NETWORKBACKUPDIR** to the **UNC** path of the network share where the backups will be copied.  
For example: **SET NETWORKBACKUPDIR=\\metropolis\musebackups**.
- Set the **MUSEBACKUPDIR** to the **UNC** path of the local drive where the backups will be saved.  
For example: **SET MUSEBACKUPDIR=d:\muse\musedbbackups**.
- Save the file.

## Configuring the Weekly Network Backup

1. Browse to **d:\muse\backup**.
2. Using an ASCII editor such as Notepad, open **Cbackup\_NO\_TAPE.bat**.
3. Change the location to the network share where the backup will be saved.

Look for the following string:

```
C:\WINDOWS\system32\ntbackup.exe backup
C:\ systemstate /v:no /j
"CDriveBackup" /m normal /l:s /f
"D:\muse\backup\CDrivebackup.bkf"
```

Change **"D:\muse\backup\CDrivebackup.bkf"** to the correct path.

For example: **"\\MUSEBkupSvr\MUSEBackup\CDrivebackup.bkf"**

4. Change the parameters for the email notification as appropriate.

Look for the following string:

```
d:\muse\backup\blat.exe
d:\muse\backup\weeklybackupstatus.txt
-subject "MUSE System Backup Status"
-to recipient@email.com
-server server.mail.com
-i "MUSESystem@muse.com"
-f sender@email.com
```

Change the following parameters as appropriate:

Parameter	Description
<b>-subject</b>	Enter the subject line for the notification email.
<b>-to</b>	Enter the email address of the notification recipient.
<b>-server</b>	Enter the name of the email server.
<b>-f</b>	Enter the email address of the notification sender.

5. Save the file.

## Configuring the Weekly Tape Backup

1. Change the destination drive if necessary.

By default, the backup job is set up to write to a Sony AIT tape drive. If you are using the **ML370 G3** platform, use the following procedure to configure the job for a Compaq AIT tape drive:

  - a. Open **d:\muse\backup\CBackup.bat** in Notepad.
  - b. In the **Eject the tape** section, comment out the **rsm** line for the Sony tape drive and un-comment the **rsm** line for the Compaq tape drive.
2. Change the tape reminder as necessary.
  - a. If not open from step 1, open **d:\muse\backup\CBackup.bat** in an ASCII editor, such as Notepad.
  - b. Edit the following parameters as appropriate:

Parameter	Description
<b>-to</b>	Enter the email address of the notification recipient.
<b>-from</b>	Enter the email address of the notification sender.
3. Save the file.

## Changing the Backup Schedule

After configuring the backup jobs [“Configuring the Backup Jobs” on page 99](#)) you can modify their scheduled start times to better suit your needs. For example, you could change the start time of the nightly backup or remove Saturday and Sunday from the backup schedule.

For a description of the default schedules, refer to [“Setting Up Automatic Backups” on page 97](#).

Use the following procedure to change the schedule for any of the jobs.

1. Open **SQL Server Management Studio** and expand **SQL Server Agent > Jobs**.
2. Right-click on the job you want to modify and select **Properties**.

3. In the left pane, select **Schedules** and click **Edit**.  
The following window opens.

4. In the **Daily Frequency** section, enter the time at which to run the job.
  - To run the job once, select the **Occurs once at** field and enter the starting time.
  - To run the job repeatedly, select the **Occurs every** field and enter the **Starting at** and **Ending at** times.
5. In the **Duration** section, enter the **Start date** and **End date** for the job.  
By default, the **No end date** option is selected. It is recommended that you keep that setting for all backup jobs.
6. Click **OK** on all open windows to close them and save your changes.

## Creating Notifications

Both network and tape backup options provide three ways to keep you informed of their status:

- **Log File**  
The MUSE backup jobs generate a log file at **d:\muse\backup\MUSEBackup**. The log file retains information only from the most recent backup: every time a backup job runs, it overwrites the previous log. Use an ASCII editor such as Notepad, to review the log file.
- **Email Notifications**  
You can configure the MUSE backup jobs to send an email with the back up log file when the backup jobs complete. In addition, if you are using the tape backup option, you can set up the system to send an email reminder to insert the backup tape.
- **Net Send Notifications**  
You can configure the MUSE backup jobs to use the Windows **Net Send** command to alert you on their status. You typically use this option to send a message when the backup job fails. It is not as reliable as email notifications; if the computer to

which you are sending the message is not online, the message is not received. This procedure is only documented here for cases where the customer wants this type of notification.

This section documents how to set up and configure the email and net send notifications.

## Email Notifications

Setting up the email notifications consists of three tasks:

- Configuring the email utility.
- Configuring the status notification.
- Configuring the tape reminder notification.

You only need to perform these tasks once.

### Configuring the Email Utility

The backup jobs use the open source **Blat** utility to send email notifications. To configure the **Blat** utility, use the following procedure:

1. Open a **Command Prompt** window and change to the **d:\muse\backup** directory.
2. Type the following command: **Blat** <space> **-install** <space> **mail.someplace.com** <space> **<sender address>**.

For example: **Blat** <space> **-install** <space> **mail.someplace.com** <space> **someone@someplace.com**.

#### NOTE:

The sender email address may be any valid email account, but customers may want to set up a special account so the MUSE backup administrator can easily identify it.

3. Press **Enter**.

A message is returned stating that the SMTP server was set to the email server address on port 25, with the user/sender address you provided, and that it is set to retry one time.

#### NOTE:

When running the **Blat** utility for the first time, you receive an error message because **Blat** needs to create registry entries. You can ignore this error.

If you need to alter the **Blat** installation settings, they are found in the following registry key - **HKLM\Software\Public Domain\Blat..**

You are now ready to configure the email notifications.

### Configuring the Status Notifications

The method for configuring the status notifications depends on the backup job.

#### Configuring the Nightly and Monthly Notifications

The nightly and monthly backup status notifications use two files:

- A batch file that contains the instructions for sending the email.
- A text file that contains the body of the email message.



Edit the files using a standard ASCII editor such as Notepad.

**NOTE:**

The monthly backup files are available only if you are using the tape backup option.

1. Open the appropriate batch file.
  - For the nightly backup, select **d:\muse\backup\nightlybackupstatus.bat**.
  - For the monthly backup, select **d:\muse\backup\monthlybackupstatus.bat**.
2. Modify the following parameters as appropriate

Parameter	Description
<b>-subject</b>	Edit this text to change the email subject.
<b>-attach</b>	Leave this value at the default.
<b>-to</b>	Enter an individual or group email address.
<b>-server</b>	Enter the address of the email server that routes the message.

3. Save the batch file.
4. Open the appropriate text file.
  - For the nightly backup, select **d:\muse\backup\nightlybackupstatus.txt**.
  - For the monthly backup, select **d:\muse\backup\monthlybackupstatus.txt**.
5. Modify the body of the email message as appropriate.
6. Save the file.

### Configuring the Weekly Notification

The weekly backup status notification is configured as part of the backup job itself. Refer to [“Configuring the Backup Jobs” on page 99](#) for details.

### Configuring the Tape Reminder Notification

The reminder to switch the backup tape is available only if you are using the tape backup option. If you are using the network backup option, skip this section.

The method for configuring the reminder depends on the backup job.

### Configuring the Weekly and Monthly Reminder

The weekly and monthly reminder use two files:

- A batch file that contains the instructions for sending the email.
- A text file that contains the body of the email message.

Edit the files using a standard ASCII editor such as Notepad.

- Open the appropriate batch file.
  - For the nightly backup, select **d:\muse\backup\nightlybackupreminder.bat**.
  - For the monthly backup, select **d:\muse\backup\monthlybackupreminder.bat**.
- Modify the following parameters as appropriate.

Parameter	Description
<b>-subject</b>	Edit this text to change the email subject.
<b>-to</b>	Enter an individual or group email address.
<b>-server</b>	Enter the address of the email server that routes the message.

- Save the batch file.
- Open the appropriate text file.
  - For the nightly backup, select **d:\muse\backup\nightlybackupreminder.txt**.
  - For the monthly backup, select **d:\muse\backup\monthlybackupreminder.txt**.
- Modify the body of the email message as appropriate.
- Save the file.

### Configuring the Weekly Reminder

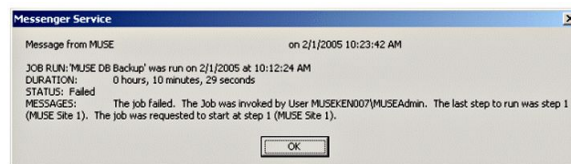
The weekly backup status notification is configured as part of the backup job itself. Refer to [“Configuring the Backup Jobs” on page 99](#) for details.

## Net Send Notifications

Configuring the Net Send notifications consists of two tasks:

- Creating and configuring the **Operator** that receives the message.
- Configuring the backup job to send the message.

After the notification is configured, you must start the **Messenger Service** on both the sending and receiving computers. Once set up, the backup sends standard Windows notifications, as seen in the following illustration.

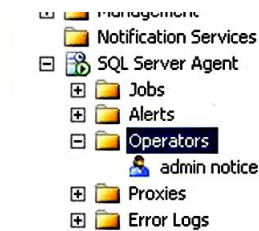


### Creating and Configuring the Operator

- Log on to the MUSE file server with a local administrator account.
- From the Windows desktop select **Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**.

The **SQL Server Management Studio** window opens.

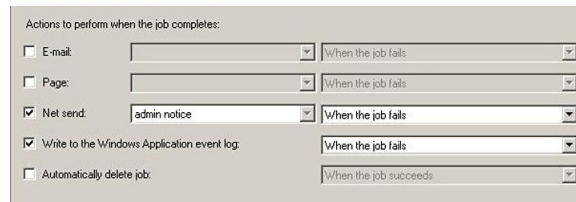
3. In the left pane, browse to **SQL Server Agent > Operators**.



4. Right-click on **Operators** and select **New Operator...** from the menu.  
The **New Operator** window opens
5. Enter the name you want to use for the **Operator** and the address of the computer you want to receive the Net Send message.
6. Click **OK** to save your changes.

### Configuring a Backup Job to Send Message

1. In the left pane of the **SQL Server Management Studio** window, browse to **SQL Server Agent > Jobs**.
2. Right-click on the backup job you want to send a **Net Send** message and select **Properties** from the menu.
3. In the left pane of the **Job Properties** window, click **Notifications**.
4. In the **Actions to perform when the job completes** section of the window, select the **Net send** check box, select the appropriate operator from the first drop-down list, and select an event from the second drop-down list.



5. Click **OK** to save your changes.
6. Exit **SQL Server Management Studio**.

## Testing the Backup Jobs

After the backup jobs have been set up and configured, run the jobs manually to ensure that they back up the data to the correct location and email the correct notifications to the correct recipient.

### Testing the Network Backup Jobs

1. Open **SQL Server Management Studio** and select **SQL Server Agent > Jobs**.
2. Right-click on the job to test, select **Start Job at Step...**, and select step 1.
  - To test the nightly backup, select the **7Nightly\_Backups** job.
  - To test the weekly backup, select the **WeeklyCDriveNetworkBackup** job.

3. After the job completes, verify that the correct files were written to the network share.
  - For the nightly backup, verify the following files were written to the network drive:
    - **[weekday]Master.bak**
    - **[weekday]MSDB.bak**
    - **[weekday]MUSE\_Site000x.bak**
    - **[weekday]SiteTemplate.bak**
    - **[weekday]System.bak**
  - Note that **[weekday]** is the day on which you ran the backup and that there is one **MUSE\_Site000x.bak** file for each site added to the MUSE system.
  - For the weekly backup, verify **CDriveBackup.bkf** was written to the network share.
4. If you are testing the nightly backup whose **COPYOPTION** parameter was set to **MIRROR** or **MIRRORSOME** (see [“Nightly Backup” on page 96](#)), verify that the backups also exists on the drive (**d:\muse\musedbbackup**).
5. Verify that the email notification was sent to the appropriate recipient and that the **musebackup.log** file was attached.
6. Verify that the attached log file is complete and accurate.
7. Refer to [“Database Recovery” on page 109](#) and verify that the backup just created can be used to restore the database.

## Testing the Tape Backup Jobs

1. Open **SQL Server Management Studio** and select **SQL Server Agent > Jobs**.
2. Right-click on the tape reminder job you want to test, select **Start Job at Step...**, and select **step 1**.
  - To test the nightly reminder, select the **NightlyBackupReminder** job.
  - To test the weekly reminder, select the **WeeklyBackupReminder** job.
  - To test the monthly reminder, select the **MonthlyBackupReminder** job.
3. Verify the email reminder to insert the backup tape was sent to the correct recipient and that it contained the correct information.
4. Insert a tape into the AIT tape drive.
 

Initialize the tape if necessary. Refer to [“Initializing a New Tape” on page 116](#) for instructions.
5. In **SQL Server Management Studio**, right-click on the backup job you want to test, select **Start Job at Step...**, and select **step 1**.
  - To test the nightly backup, select the **NightlyMUSEDDBBackup** job.
  - To test the weekly backup, select the **WeeklyMUSEDDBBackup** job.
  - To test the monthly backup, select the **MonthlyMUSEDDBBackup** job.
6. As the job runs, verify that the backup is written to the AIT tape drive.
 

Make sure the read/write light is flashing.

7. Verify that the email notification was sent to the appropriate recipient and that the ***musebackup.log*** file was attached.
8. Verify that the attached log file is complete and accurate.
9. Refer to [“Database Recovery” on page 109](#) and verify that you can use the backup just created to restore the database.

## Backing Up the Database Manually

If you need to perform a database backup between scheduled backup jobs, use the following procedure.

1. If you are using the tape backup option, insert the appropriate backup tape in the file server's tape drive.
2. Log on to the MUSE file server with the user name and password of a user with administrative privileges.
3. Open **SQL Server Management Studio**.  
The **Connect to Server** window opens.
4. In the **Server Name** list, select the server to which you want to connect.
5. Click **Connect**.
6. In the left pane of the **SQL Server Management Studio** window, browse to **SQL Server Agent > Jobs**.
7. Right-click the backup job you want to run and select **Start Job at Step....**
  - To run the nightly network backup, select **7Nightly\_Backups**.
  - To run the weekly network backup, select **WeeklyCDriveNetworkBackup**.
  - To run the nightly tape backup, select **NightlyMUSEDDBBackup**.
  - To run the weekly tape backup, select **WeeklyCDriveBackup**.
  - To run the monthly tape backup, select **MonthlyMUSEDDBBackup**.
8. Highlight **Step 1** and click **Start**.
9. Verify each step completes successfully.  
For network backups, verify that the backup files were created on the local and/or network drive and are time stamped with the date the backup ran.
10. Exit **SQL Server Management Studio** when the backup is complete.

## Database Recovery

The database recovery process is intended to restore the MUSE databases without affecting the Windows operating system, MUSE application, or the rest of the MUSE system. If the entire MUSE system becomes corrupt or unstable, use the system recovery process as described [Appendix A “System Recovery” on page 117](#).

The process to restore the database consists of the following basic tasks:

1. Copying the current databases.
2. Restoring the most recent database backup.
3. Reverting to the current database, if necessary.

Each task is described in more detail in the following sections.

## Copying the Current Database

GE Healthcare recommends that you copy the current database before restoring a backup. This allows you to back out of the restore process, if necessary, and revert to the current database.

1. Shut down all **MUSE**, **MACCRA**, and **SQL** services.
2. Navigate to **d:\muse**.
3. Right-click the **\muse\db** folder and select **Copy**.
4. Right-click in a blank area in the **\muse** folder and select **Paste**.

This creates a **\muse\Copy of db** folder.

## Recovering the MUSE Database

The process for restoring the MUSE database differs depending on whether you are using the network backup option or the tape backup option. Both processes are described in the following sections.

### NOTE:

If either restore fails, or you decide to cancel in the middle of the restore process, refer to [“Reverting to the Current Database” on page 115](#) for instructions on how to return the database to its pre-restore state.

## Recovering the MUSE Database From the Network

After creating a copy of the current **database**, use the following procedure to restore a backup of the database from the network backup.

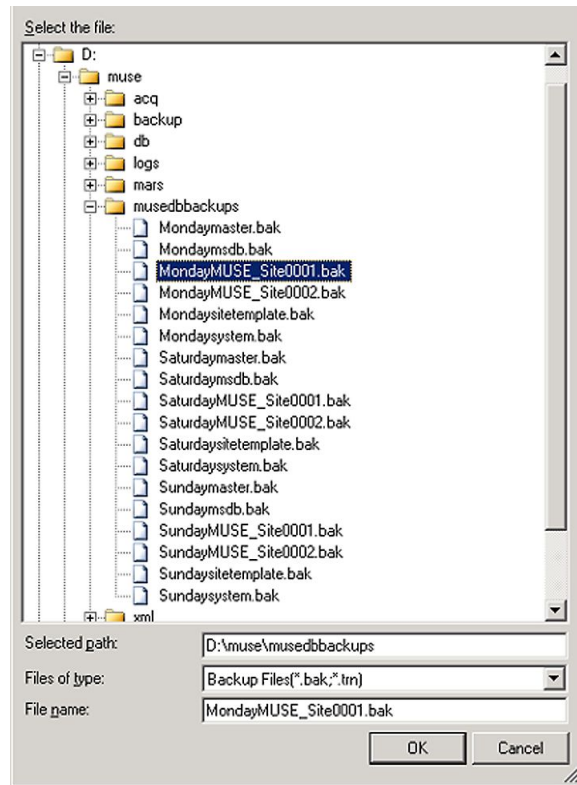
1. Log on to the MUSE server using an administrator account that has permissions to the network share where the database backups are saved.
2. Verify that all **MUSE** services and **MACCRA** are off.
3. Start the **SQL Server** and **SQL Server Agent** services.
4. Open **SQL Server Management Studio** and right-click on **Databases**.
5. Select **Restore Database**.

The **Restore Database** dialog box opens.

6. Under **Source for restore**, click the **From device** option button.
7. Select the ... button.

The **Specify Backup** dialog box opens.

8. From the **Backup Media** drop-down list, select **File** and click **Add**.  
The **Locate Backup File** dialog box opens.



9. Select the database you want to restore.
  - a. If you are restoring from the local D drive, expand the selections to **d:\muse\musedbbackup** and select the database you want to restore.
  - b. If you are restoring from the network share, enter the **UNC** path to the network share in **Selected path**. If you receive a message indicating the database engine server cannot resolve the file location and is unable to resolve the permission issue, copy the MUSE database backups from the network server to the MUSE server's **D:** drive and restore them from there.
  - c. In the **File name** field, enter the name of the database you are restoring.  
For example if you are restoring the **Monday Site 1** backup you enter **MondayMUSE\_Site0001.bak**.

10. Click **OK**.

You are returned to the **Specify Backup** dialog box with the backup location displayed.

**NOTE:**

If you are unable to save a **UNC** path, it is generally due to a permissions error. You must be logged on to the MUSE server using an account with permissions to the network share and the MUSE database on the server. You can use the **MUSEBkgnd** account for this. You may need to change the **SQLSERVER** service logon to **MUSEBkgnd** as well. If you change the logon permission for the **SQLSERVER** service, be sure to change it back to **Local System** after you are done restoring the databases; the **Local System** account is more secure. Only the **SQLServerAgent** logon account should use **MUSEBkgnd**.

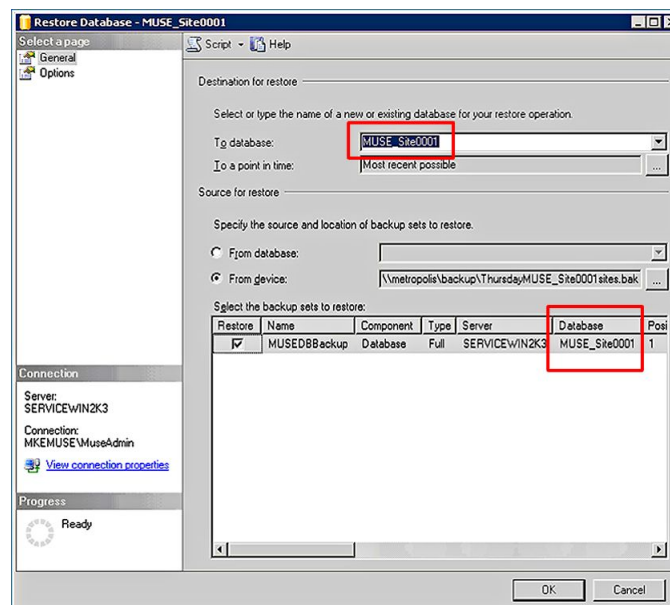
11. Click **OK**.

The **Restore Database** window opens.

12. Restore the database using the following procedure.

Note that you are restoring the **MUSE\_Site\_000x** databases first, followed by **MUSE\_SiteTemplate**, and the **MUSE\_System** database last.

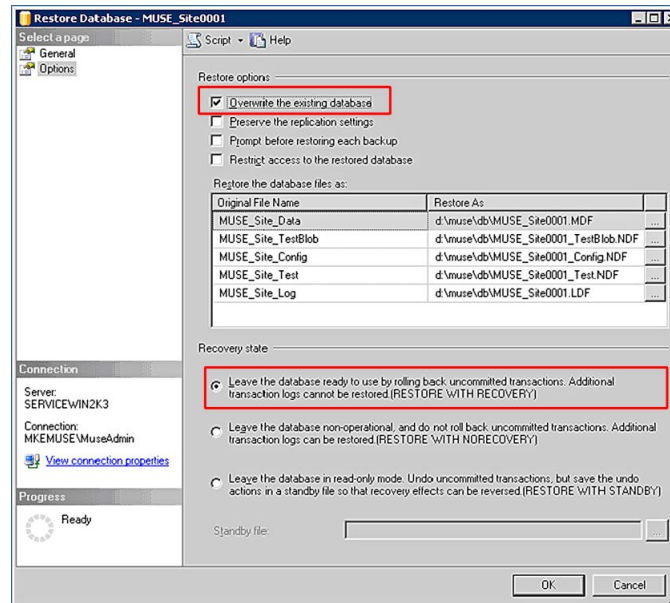
- a. Under **Select the backup sets to restore**, check the database you are restoring.
- b. Under **Destination for restore**, select the MUSE database you are restoring from the drop-down list next to **To Database**.



- c. In the left navigation pane, click **Options**.

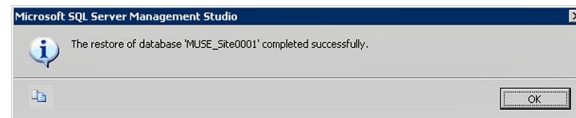


- d. In the Restore options section, select **Overwrite the existing database** and verify that **Leave the database ready for use by rolling back uncommitted transactions...** is selected in the **Restore state** section.



- e. Click **OK**.

When the database is restored, the following dialog box opens.



- f. Repeat this process for each remaining database in the order indicated at the beginning of step 12.
13. After all the databases are restored, restart the server.
- If the databases did not restore correctly, refer to [“Reverting to the Current Database” on page 115](#) for instructions on how to backup out the restored data and to revert the databases to their pre-restored state.

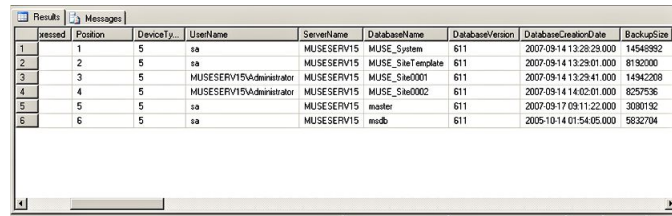
## Recovering the MUSE Database From Tape

After creating a copy of the current database, use the following instructions to restore a backup of the database from a tape backup.

1. Start the SQL Server and **SQL Server Agent** services.
2. Delete the current databases using the following procedure:
  - a. Run **SQL Server 2005 Management Studio**.
  - b. Right-click on each MUSE database and select **Delete**.
  - c. On the **Delete Object** window, select the **Delete backup and restore history information for databases** check box and click **OK**.
  - d. Repeat step b through step c for each MUSE database.
3. After the databases are deleted, insert the most recent backup tape.

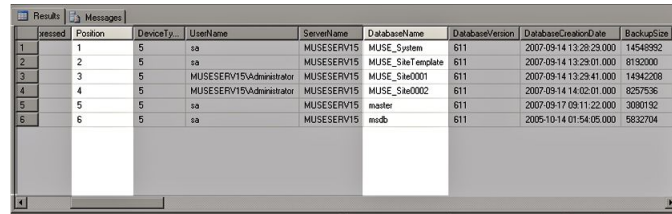
4. Click **New Query**.
5. In the query window, type the following command: **restore <space> headeronly <space> from <space> tape = <space> '\\.\tape0' <space> with <space> nounload**
6. Execute the command.

A directory of the tape's contents opens, as seen in the following illustration.



pressed	Position	DeviceType	UserName	ServerName	DatabaseName	DatabaseVersion	DatabaseCreationDate	BackupSize
1	1	5	sa	MUSESERV15	MUSE_System	611	2007-09-14 13:28:29.000	14548992
2	2	5	sa	MUSESERV15	MUSE_SiteTemplate	611	2007-09-14 13:29:01.000	8192000
3	3	5	MUSESERV15Administrator	MUSESERV15	MUSE_Site0001	611	2007-09-14 13:29:41.000	14942208
4	4	5	MUSESERV15Administrator	MUSESERV15	MUSE_Site0002	611	2007-09-14 14:02:01.000	8257536
5	5	5	sa	MUSESERV15	master	611	2007-09-17 09:11:22.000	3080192
6	6	5	sa	MUSESERV15	msdb	611	2005-10-14 01:54:05.000	5832704

7. Note the names and positions of the MUSE databases on the tape, as highlighted in the following illustration.



pressed	Position	DeviceType	UserName	ServerName	DatabaseName	DatabaseVersion	DatabaseCreationDate	BackupSize
1	1	5	sa	MUSESERV15	MUSE_System	611	2007-09-14 13:28:29.000	14548992
2	2	5	sa	MUSESERV15	MUSE_SiteTemplate	611	2007-09-14 13:29:01.000	8192000
3	3	5	MUSESERV15Administrator	MUSESERV15	MUSE_Site0001	611	2007-09-14 13:29:41.000	14942208
4	4	5	MUSESERV15Administrator	MUSESERV15	MUSE_Site0002	611	2007-09-14 14:02:01.000	8257536
5	5	5	sa	MUSESERV15	master	611	2007-09-17 09:11:22.000	3080192
6	6	5	sa	MUSESERV15	msdb	611	2005-10-14 01:54:05.000	5832704

8. In the query window, type the following restore command for each database:  
**restore <space> database <space> db\_name <space> from <space> tape <space> = <space> '\\.\tape0' <space> with <space> file <space> = <space> <position>.**

The database names and positions MUST MATCH EXACTLY what appears in the tape directory. For example, the restore commands for the databases in the previous illustrations would look like this:

**restore database MUSE\_System from tape = '\\.\tape0' with file = 1**  
**restore database MUSE\_SiteTemplate from tape = '\\.\tape0' with file = 2**  
**restore database MUSE\_Site0001 from tape = '\\.\tape0' with file = 3**  
**restore database MUSE\_Site0002 from tape = '\\.\tape0' with file = 4**

The listed sites and the positions of each database may differ with each system

9. Execute the restore commands.
10. When the restore is complete, close **SQL Server 2005 Management Studio**.
11. Restart the **MUSE**, **MACCRA**, and **SQL** services.
12. Verify the restore was successful and the database is operational and accessible, and do one of the following:
  - If the databases restored correctly, delete the **d:\muse\copy of db** folder.
  - If the databases did not restore correctly, refer to [“Reverting to the Current Database” on page 115](#) for instructions on how to back out the restored data and revert the databases to their pre-restored state.

## Reverting to the Current Database

If the restore fails, if you cancel in the middle of the restore process, or if you decide to back out the restored data, use the following instructions to revert the databases to their condition before you started the restore process.

1. Shut down all **MUSE** and **MACCRA** services.
2. Use the following procedure to delete the restored databases:
  - a. Run **SQL Server 2005 Management Studio**.
  - b. Right-click on each MUSE database and select **Delete**.
  - c. On the **Delete Object** window, select the **Delete backup and restore history information for databases** check box and click **OK**.
  - d. Repeat step b through step c for each MUSE database.
3. Copy the contents of the **d:\muse\copy of db** folder to the **d:\muse\db** folder.
4. Open a **Command Prompt** window.
5. Navigate to **c:\Program Files\muse**.
6. Type **attachmusedb** and press **Enter**.
7. Close the **Command Prompt** window.
8. Verify the MUSE databases were attached in **SQL Server 2005 Management Studio**.
9. Restart the **MUSE** and **MACCRA** services.
10. Verify the MUSE application opens and the database is present.
11. Delete the **d:\muse\copy of db** folder.

## Additional Information

When configuring or performing the system backups, you may need to shut down the system, restart the system, or initialize a new backup tape. The instructions for performing these additional tasks are provided in the following sections.

## System Shutdown and Restart Procedure

During the MUSE backup and recovery process, it may become necessary to shut down and restart the system. This section provides instructions for safely shutting down and restarting the system:

### CAUTION:

**DATA LOSS OR CORRUPTION:** Shutting down or restarting the MUSE system any way other than that specified in this manual could result in data loss or corruption.

Follow the instructions provided in this manual to shut down and restart the MUSE system.

1. Notify users that you are about to shut down the MUSE system so they can save their changes before the system is shut down.

This prevents any changes being made to open tests from being lost when the system is shut down. Records that are open when the user is disconnected

remain locked but can be unlocked by a user with the proper permissions under **Status > Locked Data List**.

2. From the Windows desktop on the MUSE server, select **Start > Shut Down**.
3. Select either of the following options:

- **Restart**

This option powers down and immediately restarts the computer.

- **Shut down**

This option powers down the computer until you manually restart it.

The MUSE services launch automatically when the server restarts and are available immediately to MUSE clients. If the system has an HL7 interface, the inbound messages queue on the HL7 server until the MUSE server is restarted.

4. After the file server is restarted, verify that all of the MUSE-related services have started and that you can run the MUSE application on the server.
5. Verify that clients are able to attach when running the MUSE application.

## Initializing a New Tape

When using an AIT tape for the first time, you must initialize it to receive data. Use the following procedure to initialize a new tape:

1. Insert a new tape into the tape drive.
2. Right-click on **My Computer** and select **Manage**.
3. Expand **Removable Storage** and select **Media**.

The tape should be listed on the right. If it is new, it displays in the **Media Pool** column as **\Unrecognized\8mm AIT 1**.

4. Highlight the new tape in the list.
5. On the menu, click **Action > Free**.

The following message opens:



6. Click **Yes**.  
Another message opens asking you to confirm that you want to make it free.
7. Click **Yes**.
8. Label the tape externally. For a nightly tape, label it **<Day> Backup**, where Day is replaced by the appropriate day of the week. For the weekly tape, label it **Weekly C: Backup**. For the monthly tape, label it **Monthly Backup**.



# System Recovery

The system recovery process restores the entire MUSE system (Windows operating system, MUSE application, MUSE databases, and supporting software) in the event it becomes corrupted or unstable. If you need to restore only the MUSE databases and not the entire system, use the database recovery process described in [“Database Recovery” on page 109](#).

You may need to recover the MUSE system for any number of reasons. The most extreme case is the loss of your disk array caused by the failure of multiple hard drives. In this case you need to:

- replace the hard drives
- configure the server as if it were new
- reinstall the MUSE system
- restore the databases

The process for restoring the MUSE system varies depending on which backup method was used:

- If you use the network backup option, see [“Server Recovery Using a Network Backup” on page 118](#).
- If you use the tape backup option, see [“Server Recovery Using a Tape Backup” on page 125](#).

**NOTE:**

Each recovery situation is different. Before performing a full system recovery, try other options to identify and resolve system failure or instability, such as restarting in Windows Safe Mode, or using the Windows Recovery Console (refer to [“Using Recovery Console” on page 117](#) for details). Performing a full system recovery should be the final resort after you have exhausted all other corrective options.

In addition to recovering the MUSE server, you can also rebuild individual MUSE clients. See [“Client Rebuild” on page 130](#) for details.

## Using Recovery Console

If Safe Mode and other startup options do not work, consider using the Recovery Console. This method is recommended only if you are an advanced user who can use basic commands to identify and locate problem drivers and files. In addition, you need the password for the built-in administrator account to use the Recovery Console.

Using the Recovery Console, you can enable and disable services, format drives, read and write data on a local drive (including drives formatted as NTFS), and perform many other administrative tasks. The Recovery Console is particularly useful if you need to repair your system by copying a file from a floppy disk or CD-ROM to your hard drive, or if you need to reconfigure a service that is preventing your computer from starting properly.

If you are unable to start your computer, you can run the Recovery Console from your Setup CD.

To start the computer and use the Recovery Console:

1. Insert the Setup CD into the optical drive and restart the computer from the CD.
2. When the text-based part of Setup begins, follow the prompts; choose the **repair** or **recover** option by pressing **R**.
3. When prompted, type the password for the local administrator account.
4. At the system prompt, type the relevant Recovery Console commands; type **help** for a list of commands or **help <space> <commandname>** for help about a specific command.
5. To exit the Recovery Console and restart the computer, type **exit**.

## Server Recovery Using a Network Backup

This system recovery procedure applies for both the HP Proliant ML370 G5 and HP Proliant DL370 G6 platforms using the network backup procedure ("[Network Backup Option](#)" on page 95).

### NOTE:

The HP Proliant ML370 G4 platform can only be recovered using ASR recovery. Refer to "[Server Recovery Using a Tape Backup](#)" on page 125.

This procedure consists of the following steps:

1. Reimaging the MUSE server.  
To reimage an HP ML370 G5 platform, refer to "[Reimaging the HP ML370 G5 Server](#)" on page 118.  
To reimage an HP DL370 G6 platform, refer to "[Reimaging the HP DL370 G6 Server](#)" on page 119.
2. Recovering the system partition (C: drive).
3. Adding the server to the domain.
4. Recovering the data partition (D: drive)
5. Restoring the MUSE databases.
6. Verifying the MUSE communications.
7. Restoring other functionality.

## Reimaging the HP ML370 G5 Server

Use the following procedure to reimage your MUSE server on an HP ML370 G5 platform. If you are recovering an HP DL370 G6 server, refer to "[Reimaging the HP DL370 G6 Server](#)" on page 119.

To configure the drive array and return the server to its base OS configuration, you need the Pre-Install and Image CDs that shipped with the hardware.

**CAUTION:**

LOSS OF DATA: Reimaging deletes all the data on the server.

Reimage the server **ONLY** if you plan to perform a complete system recovery and reinstallation of the MUSE system. If you need to restore only the MUSE database, refer to [“Database Recovery” on page 109](#).

1. Insert the MUSE Pre-Install CD into the server’s optical drive.
2. Restart the server from the CD.
3. When prompted, type **R** for a rack configuration or **T** for a tower configuration and press **Enter** to configure the drive array.  
The server restarts.
4. Remove the MUSE Pre-Install CD from the optical drive and insert the MUSE Image CD.
5. When prompted, press **Y** to continue.  
This reimages the system with Windows 2003 SP2 and SQL 2005 SP1. During the recovery of the system partition ([“Recovering the System Partition \(C: Drive\)” on page 122](#)), any service packs that were installed on the system are restored.  
When the reimage is complete, the messages **Cloning Success** and **CRC Check: Success** is displayed.
6. Remove the MUSE Image CD from the optical drive.
7. Restart the server.  
The server restarts and configures the operating system and disk partitions.  
The server restarts several times during this process. When it is complete, the **Windows logon** window opens.
8. Log on to the server as an administrator.  
If you do not know the administrator’s user name or password, contact GE Healthcare Technical Support.
9. Change the **system date** and **time** as needed.
10. Change the **computer name** to match the original name of the server.
11. Restart the server.  
Do not join the computer to the domain at this time. This step is performed after the system partition is recovered.

Proceed to [“Recovering the System Partition \(C: Drive\)” on page 122](#).

## Reimaging the HP DL370 G6 Server

Use the following procedure to reimage your MUSE server on an HP DL370 G6 platform. If you are recovering an HP ML370 G5 server, refer to [“Reimaging the HP ML370 G5](#)



[Server” on page 118](#). You need the Image CD that shipped with the hardware to configure the drive array and return the server to its base OS configuration.

**CAUTION:**

LOSS OF DATA Reimaging deletes all the data on the server.

Reimage the server ONLY if you plan to perform a complete system recovery and reinstallation of the MUSE system. If you need to restore only the MUSE database, refer to [“Database Recovery” on page 109](#).

1. Restart the server.
2. During the restart, when prompted for the **ROM-based Setup Utility** press **F9**.  
The **ROM-based Setup Utility** opens.
3. Select the **Standard Boot Order (IPL)** option and press **Enter**.  
The **Standard Boot Order (IPL)** window opens.
4. Verify that CD-ROM is listed as the first boot sequence.  
This is necessary to ensure that the system can start from the MUSE Image CD. If CD-ROM is not listed as the first boot sequence, do the following:
  - a. Use the arrow keys to select **CD-ROM** and press **Enter**.
  - b. Select **Set the IPL Device Boot Order to 1** and press **Enter**.  
The CD-ROM moves to the first position in the boot sequence.
5. Press **Esc** twice to close the menu and the **ROM-based Setup Utility**.
6. When prompted, press **F10** to confirm that you want to exit the utility.  
The system restarts and displays the following message:  
**Press F8 to run option ROM Configuration for Arrays Utility.**  
**Press ESC to skip configuration and continue.**
7. Press **F8** to run the **ROM Configuration for Arrays Utility**.
8. On the Main Menu, select **Delete Logical Drive** and press **Enter**.  
The **Delete Logical Drive** window opens.
9. In the **Available Logical Drive** section, select **F8** to delete.  
The following warning is displayed:  
**This will result in complete data loss for this logical drive. You have selected to delete logical drive #1, RAID 50, 1117.5 GB with 6 physical drive(s).**  
**Press F3 to delete the logical drive.**  
**Press ESC to cancel.**
10. Press **F3**.  
A message opens when the configuration is saved.
11. Press **Enter** to close the message window and continue.  
You return to the **Main Menu**.
12. Select **Create Logical Drive** and press **Enter**.



13. Follow the on-screen navigation instructions and verify the following settings are selected:

Field	Setting
<i>Available Physical Drives</i>	All six drives
<i>RAID Configurations</i>	RAID 50
<i>Parity Group Count</i>	2
<i>Spare</i>	Unchecked
<i>Maximum Boot Partition</i>	Disabled

14. When the settings are correct, press **Enter**.  
 The following message displays: ***You have selected a logical drive with a total data size of 1117.5 GB and RAID 50 fault tolerance.***  
***Press F8 to save the configuration.***  
***Press ESC to cancel.***
15. Press **F8**.  
 The message ***Saving Configuration*** flashes briefly.  
 When the configuration is saved, the message ***Configuration Saved*** opens.
16. Press **Enter** to close the message and continue.  
 You return to the ***Main Menu***.
17. Select the ***View Logical Drive*** option and press **Enter**.  
 The ***View Logical Drive*** window opens.
18. Verify that the window displays ***Logical Drive #1, RAID 50, 1117.5 GB***, and do one of the following:
- If everything is not correct, repeat from 13 to make the necessary changes.
  - If everything is correct, press **Esc** to return to the ***Main Menu***.
19. Insert the MUSE Image CD into the server's optical disk drive.
20. Press **Esc** to exit the ***ROM Configuration for Arrays Utility***.  
 The server restarts and the ***MARS DL370 G6 Server Image*** window opens with the following message: ***This utility will image your hard drive as a MARS Server.***  
***!!WARNING!! You are about to permanently overwrite the contents of your hard drive array. Do you wish to continue?***
21. Press **Y** to continue.  
 The system loads the ghost image and displays the message ***Loading Ghost.***  
 This process reimages the system with Windows 2003 SP2 and SQL 2005 SP3 and can take from 20 to 30 minutes to complete.  
 When the reimage is complete, the following message is displayed:  
***Imaging Results***  
***Cloning: Success***

### **CRC Check: Success**

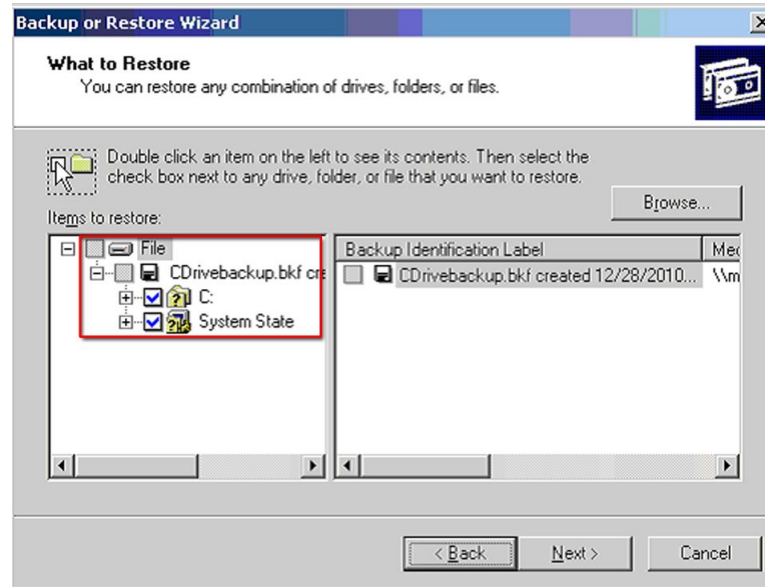
22. Remove the MUSE Image CD from the optical drive and restart the system.
  23. When the system restarts, accept the **License Agreement** and click **Next** on the remaining screens.  
The system restarts and the **HP Network Configuration Utility** opens.
  24. Click **Cancel**.  
The **HP Network Configuration Utility** closes and the system continues to boot to Windows.
  25. Log on to the server as Administrator.
  26. Adjust the **date** and **time** settings.
  27. From the desktop, select **Start > Control Panel > Add or Remove Programs**.  
The **Add or Remove Programs** window opens.
  28. Select the **Add/Remove Windows Components** option.  
The **Windows Components** window opens.
  29. Deselect **Internet Explorer Enhanced Security Configuration**.
  30. Click **Next** to save the settings.
- Proceed to ["Recovering the System Partition \(C: Drive\)" on page 122](#).

## **Recovering the System Partition (C: Drive)**

After reimaging the server ("Reimaging the HP ML370 G5 Server" on page 118 or "Reimaging the HP DL370 G6 Server" on page 119) use the following procedure to restore the system partition.

1. Log on to the MUSE server as Administrator, if necessary.
2. Create an account with read/write permissions to the network share where the weekly C: drive backup is stored and add it to the **Administrators** users group.
3. Log off the MUSE server and log back on using the account you just created.
4. On the MUSE desktop, select **Start > Run** to open the **Run** dialog box.
5. Type **ntbackup** and click **OK**.  
The **Backup or Restore Wizard** window opens.
6. Click **Next**.  
The **Backup or Restore** dialog box opens.
7. Select **Restore Files and Settings**.
8. Click **Next**.  
The **What to Restore** dialog box opens.
9. Click the **Browse** button.  
The **Open Backup File** dialog box opens.
10. Enter the network path and name of the C: drive backup file.  
For example: **\\servername\share\cDriveBackup.bkf**.

11. Click **OK**.  
The **Open Backup File** dialog box closes and you return to the **What to Restore** dialog box.
12. Under **Items to Restore**, expand the **File** and **cDriveBackup** selections and verify the backup file date being restored is correct.
13. Select the **C:** and **System State** check boxes.



14. Click **Next**.  
The **Completing the Restore Wizard** dialog box opens.
15. Click **Advanced** and do the following:
  - a. Under **Restore files to**, select **Original Location** and click **Next**.
  - b. Click **OK** at the warning.
  - c. Under **How to restore**, select **Replace existing files** and click **Next**.
  - d. Under **Advanced Restore Option**, do the following:
    - i. Select **Restore security settings**.
    - ii. Select **Preserve existing volume mount points**.
    - iii. Clear the remaining check boxes
  - e. Click **Next**.
16. Review your settings on the **Completing the Restore Wizard** dialog box and click **Finish**.  
The **Restore Progress** window opens.
17. When the **Complete** status displays, close the window and restart the computer.  
Proceed to ["Adding the Server to the Domain"](#).

## Adding the Server to the Domain

After the system is restarted it may already belong to a domain; however, the domain user accounts may display the **Security Identifier (SID)** instead of the **domain\user name**.

To check, open a **Windows group** that has domain user accounts, such as the Administrator or MUSE Web Users Group. If the **SID** is displayed instead of the user names, try generating new **SIDs**, by removing the computer from the domain and adding it again using the following the procedure.

1. Add the computer to a **workgroup** and restart the system to save the changes.
2. Add the computer to the **domain** and restart the system to save the changes.
3. Verify that any **domain accounts** under **Windows groups** are now recognized.

Examples may include **domain\MUSEAdmin** and **domain\MUSEBkgnd** accounts under the Administrators group and **domain\user** accounts under the MARS Web Users group. If the **domain\users** are still not displaying properly, you may need to add them again manually.

Proceed to [“Recovering the Data Partition \(D: Drive\)”](#).

## Recovering the Data Partition (D: Drive)

After the computer IS added to the domain [“Adding the Server to the Domain”](#) on page 123 use the following procedure to restore the data partition.

1. Log on to the server using the Administrator account.
2. Create the following file structure on the D: drive:

```
D:\
  Muse\
    acq\
    backup\
    db\
    logs\
    mars\
    xml\
```

3. If you are using **XML Import**, copy the **\*.dtd** files from the **musedb\dtd** folder on the **MUSE Application CD** to **d:\muse\xml** on the server.
4. Copy the files from the **Local Tape Backup** folder on the **MUSE Application CD** to **d:\muse\backup** on the MUSE server.

This allows you to reconfigure the backup files again after the database is restored.

5. Use the following procedure to share the **acq** folder.
  - a. Right-click on the **acq** folder and select **Properties**.
  - b. Click the **Sharing** tab.
  - c. Type **acq\$** as the share name.
  - d. If the customer is using CASE to MUSE communications, click **New Share**, enter **case8000** in the **Share Name** field, and click **OK**.
  - e. Click **Permissions**, add the **MUSE Acq Users** group, grant it **Change and Read** permissions, and click **OK**.

Proceed to [“Restoring the MUSE Databases”](#).

## Restoring the MUSE Databases

The process for restoring the MUSE databases during a system recovery is identical to the database recovery process. See [“Recovering the MUSE Database From the Network” on page 110](#) for details.

## Verifying the MUSE Communications

After the MUSE databases are restored, verify that you can perform the following actions as required by the original system configuration.

- You can launch the MUSE application from the server.
- You can access the MUSE application from a client and acquire a patient test.
- MUSE can receive an ECG from a cart through wireless or LAN (Serial IP).
- MARS to MUSE communication works.
- CASE\Cardiosoft to MUSE communication works.
- GE Healthcare Technical Support can remotely access the system using the InSite ExC services.
- The MUSE system can communicate to the CCG server, if the system has HL7 interface.
- Web client can access the web server, if the system has MUSE Web.
- Web client can access the web server, if the system has CV Web.

## Restoring Other Functionality

If any of the communication checks ([“Verifying the MUSE Communications”](#)) fail, you may need to reinstall and reconfigure device communications and perform basic MUSE system troubleshooting.

If the customer is using the **XML import** option, share **d:\muse\xml** as described in [“Installing and Configuring the XML Import Option” on page 48](#).

Recreate and configure the backup jobs as described in [“Setting Up Automatic Backups” on page 97](#).

## Server Recovery Using a Tape Backup

This system recovery procedure applies for both the HP Proliant ML370 G4 and HP Proliant ML370 G5 platforms using the local tape backup procedure (refer to [“Local Tape Backup Option” on page 97](#)).

This procedure consists of the following steps:

1. Using Automated System Recovery
2. Configuring the file server RAID array
3. Recovering the system partition (C: drive)
4. Recovering the MUSE databases
5. Performing other system tasks

## Using Automated System Recovery

There are several reasons why you might need to perform a disaster recovery. This procedure describes a situation where you have replaced multiple failed hard drives and need to start configuring the server as if it were new.

Another disaster recovery situation may be different, so you should use this information as a guide to help you recover a system. For example, you may not need to reconfigure the RAID 5 drive array.

### NOTE:

To perform an Automated System Recovery (ASR), you need the automated system recovery media, typically created by GE Healthcare service personnel during installation or system maintenance, and the floppy disk created with that media. You cannot use a floppy disk created at a different time or with a different set of media.

Make sure you have the following before you begin the recovery procedure:

- Your most recent ASR media set (floppy disk and AIT tape).
- A Windows Server 2003 CD.
- The most recent MUSE database backup tape.
- **370G5 MUSE Pre-Install CD** (G5 platforms only)

## Configuring the File Server RAID Array

The process for configuring the file server's RAID array differs depending on whether your system is running on a G4 platform or a G5 platform.

### Configuring the File Server RAID Array on a G4 Platform

1. Power-up the system.
2. When the prompt **Press F8 to run the Option ROM Configuration for Arrays Utility** is displayed, press **F8**.
3. Highlight **Delete Logical Drive** and press **Enter**.
4. Do one of the following:
  - If the **There are no available logical drives** screen opens, press **Esc** and skip to 5.
  - If logical drives exist, do the following:
    - a. Press **F8** to delete the logical drives.
    - b. On the **Warning** window, press **F3**.
    - c. On the **Configuration saved** window, press **Enter**.
5. Highlight **Create Logical Drive** and press **Enter**.
6. In the **Available Physical Drives** box, select the last drive and press the **spacebar** to remove the drive from the array.
7. Verify **RAID 5** is selected.
8. Press the **Tab** key twice to select **Use one drive as spare** and press the **spacebar**. Verify that the letter **S** is displayed in the check box.
9. Press **Enter** to create the drive.
10. Press **F8** to save the configuration.

11. Press **Enter** on **Configuration Saved** window.
  12. On the **Main Menu** window, press **Esc** to exit and resume the boot process.
- NOTE:**  
Normally you do not need to do the next set of steps if the system was already running MUSE v7, but they might be necessary, depending on what hardware was replaced on the file server.
13. Press **F9** when the message **Press "F9" key for ROM-Based Setup Utility** opens.
  14. Select **System Options** and press **Enter**.
  15. If **OS selection** is present, perform the following steps:
    - a. Select **OS selection** and press **Enter**.
    - b. Select or verify **Microsoft Windows 2000/Windows Server 2003** as the O/S to install. (This may show as **Microsoft Windows 2000/Windows .NET**.)
    - c. Press **Enter**.
    - d. Press **Esc**.
  16. Select **Boot controller Order** and press **Enter**.
  17. Select or verify **Smart Array controller** and press **Enter**.  
Depending on the server, the array could be labeled **400**, **641**, or **643**.
  18. Select **Controller Order 1** and press **Enter**.
  19. Press **Esc**.
  20. Select **Date and Time** and press **Enter**.
  21. Enter the current date and time and press **Enter**.
  22. Select **Advanced Options** and press **Enter**.
  23. If **Post F1 Prompt** is present, perform the following steps:
    - a. Select **Post F1 Prompt** and press **Enter**.
    - b. Select **Disabled** and press **Enter**.
    - c. Press **Esc** twice.
  24. Press **F10** to confirm current boot controller is **Compaq Smart Array (641 or 642) Controller**.  
The system restarts.

When the system restarts, proceed to ["Recovering the System Partition" on page 128](#).

## Configuring the File Server RAID Array on a G5 Platform

1. Power-up the system.
2. When the prompt **Press F8 to run the Option ROM Configuration for Arrays Utility** is displayed, press **F8**.
3. Highlight **Delete Logical Drive** and press **Enter**.

4. Do one of the following:
  - If the **There are no available logical drives** window opens, press **Esc** and skip to 5.
  - If logical drives exist, do the following:
    - a. Select the drive with the highest number.  
For example, if the logical drives are Drive 0 and Drive 1, delete Drive 1 before deleting Drive 0.
    - b. Press **F8** to delete the selected drive.
    - c. On the warning window, press **F3**.
    - d. On the **Configuration Saved** window, press **Enter**.
    - e. Repeat a through d for each logical drive
5. Insert the **370G5 MUSE Pre-Install CD** into the optical drive.
6. On the **Option ROM Configuration for Arrays Utility** main menu, press **Esc** to restart the server.  
The system restarts from the CD.
7. When prompted, press **R** for Rack or **T** for Tower, whichever is appropriate for the platform, and press **Enter**.  
The drive array is configured. When it is done, the system automatically restarts.
8. Remove the CD from the optical drive.

Proceed to [“Recovering the System Partition” on page 128](#)”.

## Recovering the System Partition

1. Insert the **Windows Server 2003 Recovery CD** into your optical drive and the **ASR AIT Tape** into the tape drive.
2. Restart your computer.  
The computer should start from the CD. If it does not, check the boot order in the BIOS setup.
3. When the **F6** prompt is displayed at the bottom of the **Windows Setup** window, press **F6**.
4. When you are prompted to run the **Automated System Recovery (ASR)**, press **F2**.
5. When prompted, insert the **ASR** floppy disk into the diskette drive and press **Enter**.
6. When the system prompts you for the floppy drive with the tape driver, press **S**.  
**NOTE:**  
If the SDX-550V tape driver was not added to the ASR floppy when it originally created, you need to copy it onto a floppy disk from the hardware Support CD that shipped with the system before pressing the **S** key.
7. When you are prompted to select the driver to install, select **Sony AIT - SAIT 32 Bit Tape Driver for Windows Server 2003** and press **Enter**.
8. When **Windows Setup** prompts you for additional device drivers, press **Enter** to continue.



9. When prompted to delete and recreate the disk partitions, press **C** to continue.  
The drive is formatted and setup files are copied to the **Windows installation** folders. When it is done, the system restarts and the normal Windows installation continues. When Windows is installed, the **Automated System Recovery** process starts.
10. Follow the prompts to allow the system to restore from the ASR tape.  
When the process is complete, the system restarts. At this point, the original **C:** drive is restored from the ASR tape. This process does not restore the MUSE database. You must restore the databases separately.

Proceed to ["Recovering the MUSE Databases"](#).

## Recovering the MUSE Databases

The process of recovering the MUSE database consists of three basic steps:

1. Formatting the D: partition.
2. Installing the default MUSE databases.
3. Restoring data from the most recent backup tape.

Each step is described in more detail in the following topics.

### Formatting the D: Partition

1. Sign on to the server as an administrator.
2. Shut down all **MUSE** and **MACCRA** services.
3. Run the **Microsoft SQL Management Studio**.
4. Right-click on each MUSE database and select **Delete**.
5. On the **Delete Object** window, select the **Delete backup and restore history information for databases** check box and click **OK**.
6. Repeat 4 through 5 for each MUSE database.
7. Close the **Microsoft SQL Management Studio**.
8. Right-click on **My Computer** and select **Manage**.
9. On the **Computer Management** window, select **Storage > Disk Management**.
10. Right-click on drive D: and select **Format....**
11. On the **Format** window, verify the **File System** is set to **NTFS** and the **Perform a Quick Format** check box is selected.
12. Click **OK**.
13. When the warning message appears, click **OK**.  
The system begins formatting the D: partition. When it is done, you have a clean D: drive and its status is changed to **Healthy**.

Continue to ["Installing the Default MUSE Databases"](#).

### Installing the Default MUSE Databases

1. Log on using the **MUSEAdmin** account.
2. Insert the MUSE Application CD into the optical drive.
3. Open a **Command Prompt** window and change to the **x:\musedb** directory, where x: is the CD-ROM drive letter.

4. Type **install** and press **Enter**.
5. Respond to the **License Agreement** prompt.

The system installs the default databases and any ancillary files.

When the installation is done, proceed to [“Restoring From the Most Recent Backup Tape”](#).

## Restoring From the Most Recent Backup Tape

The process for restoring the MUSE databases during a system recovery is identical to the database recovery process. See [“Recovering the MUSE Database From Tape” on page 113](#) for details.

## Other Tasks to Perform After System Restore

- If the customer is acquiring CASE data over the network, you need to perform the following steps.
  - a. Right-click on the folder in **Windows Explorer** and select **Sharing and Security...**
  - b. Select **Share this folder**.
  - c. Change the share name to **acq\$** and click on the **Permissions** button.
  - d. Remove the **Everyone** group, and add the local **case8000** user.
  - e. Give the **case8000** user **Change and Read** permissions.
  - f. If Stress systems were already copying data to this folder, you may also need to share the folder as “case8000” if that is how the Stress systems are configured.
- If the customer is using the **XML import** option, share the **d:\muse\xml** folder as described in [“Installing and Configuring the XML Import Option” on page 48](#).
- If the system was configured with the **MUSE Web** option, verify and, if necessary, reinstall MUSE Web. See the **MUSE v8 Cardiology Information System Devices and Interfaces Manual** for detailed procedures.
- Recreate any backup jobs as described in [“Setting Up Automatic Backups” on page 97](#).

## Client Rebuild

The HP rp5800 platform is available in the following configurations:

MUSE Client	Operating System	OS Edition
MUSE v7	Windows XP	32-bit
MUSE v8	Windows XP	32-bit
	Windows 7	32-bit
		64-bit <sup>1</sup>

The re-imaging process varies slightly depending on the platform’s operating system. You may only re-image a system with the same operating system with which it was

1. You cannot use the 64-bit edition of Windows 7 if the MUSE client will have a physical modem attached for the acquisition of ECGs. The modem service required for this function does not support it.

shipped. To identify the operating system, refer to the Windows tag located on the side or top of the device.

**NOTE:**

As a result of additional security measures implemented by Microsoft with Windows 7, the built-in Windows **Administrator** account is disabled by default when the operating system is installed. You will be prompted to provide a user name and password when you reboot the system during the Windows configuration process that follows re-imaging. That user will be added as a local administrator on the system.

The rebuild process consists of the following tasks:

1. Setting SATA emulation and boot order.
2. Loading the image.
3. Configuring the operating system.
4. Activating the operating system.

**NOTE:**

Activating Windows requires access to a phone line. Network and Internet access is not set up during the re-imaging process.

5. Reinstalling the MUSE application.

Each task is described in the detail in the following sections.

## Setting SATA Emulation and Boot Order (All Configurations)

Use the following procedure to verify and, if necessary, set the system's SATA emulation mode and boot order to ensure the platform boots from the image CD in the next procedure. This procedure is identical regardless of the platform's operating system.

1. Boot the computer.
2. While the computer boots, press and hold **F10** until the **Hewlett-Packard Computer Setup** utility opens.
3. Select **Storage > Storage Options** and press **Enter**.  
The **Storage Options** window opens.
4. Verify the **SATA Emulation** field is set to **IDE Mode**.  
If it is not set to **IDE Mode**, you will receive the error "**Bad Command or Filename**" when you attempt to image the system.
5. Do one of the following:
  - If the **SATA Emulation** field is set to **IDE Mode**, press **Esc** to close the **Storage Options** window without making any changes.
  - If **SATA Emulation** is not set to **IDE Mode**, do the following:
    - a. Press the down arrow key to move the cursor to the **SATA Emulation** field.
    - b. Press the right arrow key until **IDE Mode** is selected.

**NOTE:**

When you first press the right arrow key, a message opens to warn you that changing SATA emulation may prevent access to the hard drives and degrade or corrupt the current volumes. Press **Enter** to close the message.

- c. When **IDE Mode** is displayed, press **F10** to accept the change.  
The **Storage Options** window closes, and you return to the **Storage** menu.
6. Select **Storage > Boot Order** and press **Enter**.  
The **Boot Order** window opens.
7. Verify the boot devices listed under **Legacy Boot Sources** are in the following order:
  - ATAPI CD/DVD Drive
  - Hard Drive
    - SATA0
    - USB Hard Drive
  - USB Floppy/CD
  - Network Controller

**NOTE:**  
The GE configuration for the rp5800 does not use EFI boot sources.
8. Do one of the following:
  - If the boot order is correct, press **Esc** to close the **Boot Order** window without making any changes.
  - If the boot order is incorrect, do the following:
    - a. Press the down arrow key to move the cursor to the boot device to be moved.
    - b. Press **Enter** to select the boot device.
    - c. Press the up and down arrow keys to move the selected boot device to the correct position in the list.
    - d. When the boot device is in the correct position, press **Enter** to deselect it.
    - e. Repeat step a through step d until all the boot devices are in the correct order.
    - f. When the boot order is correct, press **F10** to accept the changes.  
The **Boot Order** window closes, and you return to the **Storage** menu.
9. Select **File > Save Changes and Exit** and press **Enter** to save your changes.  
The **Save Changes and Exit** window opens and prompts you to confirm that you want to save your changes and exit the setup utility.
10. Select **Yes** and press **Enter**.  
Your changes are saved, the **Hewlett-Packard Computer Setup** utility closes, and the system reboots. Proceed to ["Loading the Image"](#).

## Loading the Image

Use the following procedure to load the factory image onto the HP rp5800 platform.

1. Insert the image media into the system's optical drive.  
The following table identifies which media to use.

Operating System	OS Edition	Image Part Number
Windows XP	32-bit	2070642-003
Windows 7	32-bit	2070642-001
	64-bit	2070642-002

2. Reboot the computer.

The system boots to the System Image screen, which warns you that you are about to permanently overwrite the contents of the hard drive and asks if you want to continue.

3. Press **Y**.

The image begins to load onto the computer. When it is done, it verifies the image was applied successfully and displays the following status message:

Imaging Results:

Cloning: Success

CRC Check: Success

4. Remove the image CD from the optical drive.
5. Proceed to the correct procedure for configuring the operating system that was imaged.
  - For Windows XP Professional, proceed to [“Configuring Windows XP” on page 133](#).
  - For Windows 7, proceed to [“Configuring Windows 7” on page 134](#).

## Configuring the Operating System

After loading the image, you must configure the operating system. The configuration procedure varies slightly depending on the platform’s operating system. Use the correct procedure for the operating system of your platform.

### Configuring Windows XP

Use the following procedure to configure the Windows XP Professional operating system on your MUSE client.

1. Reboot the computer.  
When the computer reboots, the **Windows XP Professional Setup** window opens.
2. Click **Next**.  
A license agreement window opens.
3. Select the **I accept this agreement** option and click **Next**.  
A window opens with the regional and language settings. The defaults are United States and English.
4. Change the regional and language settings as required and click **Next**.  
A window opens to prompt for the hospital name and organization.

5. Enter the hospital name and organization specified by the customer and click **Next**.  
The **Your product key** window opens.
6. Enter the product key, found on the Windows label attached to the computer, and click **Next**.  
A window opens with the default computer name.
7. Change the computer name as necessary and click **Next**.  
A window opens to prompt for the password for the local administrator account. This will be the password required to log on to the administrator account after the computer reboots.
8. Enter a password for the administrator account and click **Next**.  
The **Review your time and date settings** window opens.
9. Adjust the date and time, if needed, make sure the **Automatically adjust clock for Daylight Saving Time** check box is checked, and click **Next**.  
The system performs a series of setup tasks. When the setup tasks are complete, the computer reboots and the **Logon** window opens with the **Administrator** account selected by default.
10. Enter the Administrator password set in step 8 and click **OK**.  
The Windows desktop opens.
11. Verify the desktop opened without errors.
12. Proceed to ["Activating Windows XP" on page 136](#).

## Configuring Windows 7

Use the following procedure to configure the Windows 7 operating system on your MUSE client.

1. Reboot the computer.
2. While the computer reboots, press and hold **F10** until the **Hewlett-Packard Computer Setup** utility opens.
3. Select **Storage > Storage Options** and press **Enter**.  
The **Storage Options** window opens.
4. Change the **SATA Emulation** field to **AHCI Mode**.  
Windows 7 requires AHCI Mode in order to boot. If any other **SATA Emulation** mode is selected, the system will repeatedly boot into the **Windows Recovery** screen.  
Use the following procedure:
  - a. Press the down arrow key to move the cursor to the **SATA Emulation** field.
  - b. Press the right arrow key until **AHCI Mode** is selected.

### NOTE:

When you first press the right arrow key, a message opens to warn you that changing SATA emulation may prevent access to the hard drives and degrade or corrupt the current volumes. Press **Enter** to close the message.

- c. Verify the **eSATA Port** is set to **Disabled**.
  - d. Press **F10** to accept the change.  
The **Storage Options** window closes, and you return to the **Storage** menu.
  - e. Select **File > Save Changes and Exit** and press **Enter**.  
The **Save Changes and Exit** window opens and prompts you to confirm that you want to save your changes and exit the setup utility.
  - f. Select **Yes** and press **Enter**.  
Your changes are saved, the **Hewlett-Packard Computer Setup** utility closes, and the computer reboots. After the computer reboots, the **System Setup** window opens.
5. Verify the **Country or region**, **Time and currency**, and **Keyboard Layout** are correct.  
Change any value as necessary.
  6. Click **Next**.  
A window opens and prompts you to enter a user and computer name. This user will be the set up as the local administrator.
  7. Enter the user and computer name and click **Next**.  
A window opens to prompt for the user account password. This will be the password required to log on to the administrator account after the computer reboots.
  8. Enter a user password and password hint, and click **Next**.  
The **Type your Windows product key** window opens.
  9. Enter the product key from the Windows label attached to the computer.
  10. Clear the **Automatically activate Windows when I'm online** check box.
  11. Click **Next**.  
The **Please read the license terms** window opens.
  12. Select the **I accept the license terms** check box and click **Next**.  
The **Help protect your computer...** window opens.
  13. Select **Ask me later** and click **Next**.  
The local IT administrator must determine how Microsoft updates should be installed. These settings can be adjusted later.  
The **Review your time and date settings** window opens.
  14. Adjust the date and time settings, if needed, and make sure the **Automatically adjust clock for Daylight Saving Time** check box is checked.
  15. Click **Next**.  
One of two things happens.
    - If the **Windows Activation** window opens, go to step 16.
    - If the logon screen opens with a listing of the user accounts that have been set up on the system, skip to step 17.

16. If the **Windows Activation** window opens, do the following:
  - a. Select **Activate now**.  
A list of activation options is displayed.  
**NOTE:**  
If you select **Ask me later**, the next time you start Windows you may receive the an error message stating that are not running a genuine copy Windows. If you choose to activate Windows later, see [“Activating Windows 7” on page 137](#) for instructions.
  - b. Select the **Automated phone system** option and follow the instructions to activate Windows.
  - c. When the activation is complete, reboot the computer.  
After the computer reboots, a logon screen opens and displays the user accounts that have been set up on the system is displayed.
17. Select the user account defined in step 7, enter the password defined in step 8, and click **OK**.  
The Windows desktop opens.
18. Verify the desktop opened without errors.
19. Proceed to [“Activating Windows 7” on page 137](#).

## Activating the Operating System

After configuring the operating system, you must activate it. The activation procedure varies slightly depending on the platform's operating system. Use the correct procedure for the operating system of your platform.

### Activating Windows XP

Use the following procedure to activate your Windows XP system.

1. From the Windows desktop, select **Start > Activate Windows**.  
The **Activate Windows** window opens.
2. Select the appropriate activation option.
  - To activate Windows over the Internet, select **Yes, let's activate Windows over the Internet now**.
  - To activate Windows over the telephone, select **Yes, I want to telephone a customer service representative to activate Windows**.
3. Click **Next** and follow the on-screen instructions to complete the activation.
4. When the activation is complete, proceed to [“Reinstalling the MUSE Application” on page 137](#).



## Activating Windows 7

If you did not select **Activate Now** while configuring Windows 7, use the following procedure to activate your Windows 7 system now.

1. Use the following procedure to open the **Activate Windows now** window:
  - a. On the Windows desktop, select **Start**.  
The **Start** menu opens.
  - b. Right-click on **Computer**.  
A context menu opens.
  - c. Click **Properties**.  
The system control panel opens.
2. Select the appropriate activation option.
  - To activate Windows over the Internet, do the following:
    - a. Click **Activate Windows now**.
    - b. Click **Activate Windows online now**.
  - To activate Windows over the telephone, do the following:
    - a. Click **Activate Windows now**.
    - b. Click **Show me other ways to activate**.
    - c. Click **Use the automated phone system**.
3. Follow the on-screen instructions to complete the activation.
4. When the activation is complete, proceed to ["Reinstalling the MUSE Application" on page 137](#).

## Reinstalling the MUSE Application

After the operating system has been configured and activated, you are ready to reinstall the MUSE application. Refer to the *MUSE™ Cardiology Information System Client Installation Instructions* for details.





# Electromagnetic Compatibility

The information in this section is based on current OEM information at the time of publication. GE Healthcare is not responsible for changes to information by OEM. For more details, refer to the OEM website for your equipment.

## Electromagnetic Compatibility for DL370 G6 Server

The MUSE DL370 G6 server fulfills the requirements of the following directives, standards, and normative documents:

- FCC 47CFR Part 15: Title 47—Telecommunication CHAPTER 1—FEDERAL COMMUNICATIONS COMMISSION PART 15—RADIO FREQUENCY DEVICES
- Medical Devices Directive (MDD): Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ No L 169/1 of 1993-07-12)

## Electromagnetic Compatibility (EMC) Requirements

### Electromagnetic Compatibility (EMC) Requirements

<p>EMC directive compliance used to support GEMS-IT information technology equipment (ITE) used in a medical device/system when the device:</p> <ul style="list-style-type: none"><li>• Complies with applicable international EMC standards.</li><li>• A risk analysis/assessment has determined the EMISSIONS and/or IMMUNITY of the ITE equipment shall not adversely affect the <b>essential performance</b> or <b>safety</b> of the SYSTEM.</li><li>• The EMISSIONS of the ITE equipment shall not cause the EMISSIONS of the SYSTEM to exceed applicable limits.</li></ul>	<b>EMI/EMC – Medical (Emissions and Immunity)</b>	
	EN 60601-1-2:2007 (IEC 60601-1-2:2007 (Modified))	Medical electrical equipment — Part 1-2: General requirements for safety—Collateral standard: Electromagnetic compatibility – Requirements and tests
	• Per Annex G	Guidance for determining if non-medical electrical equipment used in a SYSTEM is exempt from the EMC testing requirements of this standard.
	EMC Directive: Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to Electromagnetic Compatibility (OJ L 139/19 of 1989-05-23)	
	<b>EMI/EMC – Emissions (Radiated, RF)</b>	
	EN 55022:2006, +A1:2007 (CISPR 22:2005, +A1:2005 (Modified))	Information technology equipment — Radio disturbance characteristics — Limits and methods of measurement
	<b>EMI/EMC — Emissions (Conducted, AC Mains)</b>	

## Electromagnetic Compatibility (EMC) Requirements (cont'd.)

EN 61000-3-2:2006,+A1:2009, +A2:2009 (IEC 61000-3-2:2005, +A1:2008, +A2:2009)	Electromagnetic compatibility (EMC) — Part 3-2: Limits — Limits for harmonic current emissions (equipment input current up to and including 16 A per phase)
EN 61000-3-3:2008 (IEC 61000-3-3:2008)	Electromagnetic compatibility (EMC) — Part 3-3: Limits; Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current less than or equal to 16 A per phase and not subject to conditional connection
<b>EMI/EMC — Immunity</b>	
EN 55024:1998, +IS1:2007 (CISPR 24:1997, +A1:2001, +A2:2002 (Modified))	Information technology equipment — Immunity characteristics — Limits and methods of measurement
• EN 61000-4-2:2009 (IEC 61000-4-2:2008)	Electromagnetic Compatibility (EMC) — Part 4-2: Testing and Measurement Techniques — Electrostatic Discharge Immunity Test
• EN 61000-4-3:2006, +IS1:2009	Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test
• IEC 61000-4-4:2004, +A1:2010	Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques — Electrical fast transient/burst immunity test
• EN 61000-4-5:2006 (IEC 61000-4-5:2005)	Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques; Surge immunity test
• EN 61000-4-6:2009 (IEC 61000-4-6:2008)	Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields
• IEC 61000-4-8:2009	Electromagnetic Compatibility (EMC) — Part 4-8: Testing and Measurement Techniques — Power Frequency Magnetic Field Immunity Test
• EN 61000-4-11:2004 (IEC 61000-4-11:2004)	Electromagnetic compatibility (EMC) — Part 4-11: Testing and measurement techniques — Voltage dips, short interruptions, and voltage variations immunity tests

**NOTE:**

The MUSE DL370 G6 server is EN 55022, EN 55024, EN 61000-3-2, EN61000-3-3 and FCC compliant as declared by the OEM, HP. GE Healthcare installs only one component to the system. It is deemed relative equivalent to other HP components install. See DOC0833976, Appendix A for details. GE Healthcare system is defined as a subset of the HP evaluated system.

## Guidance and Manufacturer's Declaration–Electromagnetic Emissions

The MUSE DL370 G6 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL370 G6 server should assure that it is used in such an environment.

### Guidance and Manufacturer's Declaration–Electromagnetic Emissions

Emissions Test	Compliance	Electromagnetic Environment-Guidance	Objective Evidence
RF emissions (Radiated) <ul style="list-style-type: none"> <li>30 MHz to 1,000 MHz IEC 60601-1-2 EN 55022 (CISPR22)</li> <li>30 MHz to 5 GHz FCC 47CFR Part 15.33 FCC 47CFR Part 15.109</li> </ul>	Group 1 Class B	<b>Group 1 use</b> The MUSE DL370 G6 server uses RF energy only for its internal function. Therefore, its RF emissions are very low and are not likely to cause any interference in nearby electronic equipment.	NOTE 3
RF emissions (Conducted) <ul style="list-style-type: none"> <li>150 KHz to 30 MHz IEC 60601-1-2 EN 55022 (CISPR22)</li> <li>150 KHz to 30 MHz FCC 47CFR Part 15.107</li> </ul>	Group 1 Class B	<b>Class B use</b> The MUSE DL370 G6 server is suitable for use in all establishments, including domestic establishments and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes.	NOTE 3
Harmonic Emissions 2nd – 40th Harmonic IEC 60601-1-2 EN/IEC 61000-3-2	Class D	The MUSE DL370 G6 server is suitable for use in all establishments, including domestic establishments and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes.	NOTE 4
Voltage fluctuations/ Flicker emissions IEC 60601-1-2 EN/IEC 61000-3-3	Complies Pass		NOTE 4
<p>NOTE 1: At 80 MHz and 800 MHz, the higher frequency range applies.</p> <p>NOTE 2: These guidelines may not apply in all situations. Electromagnetic propagation is affected by reflection from structures, objects, and people.</p> <p>NOTE 3: See TR09157.pdf (part of DOC0723504).</p> <p>NOTE 4: See DOC0836172.</p>			

## Guidance and Manufacturer's Declaration–Electromagnetic Immunity

The MUSE DL370 G6 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL370 G6 server should assure that it is used in such an environment.

## Guidance and Manufacturer's Declaration–Electromagnetic Immunity

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment – Guidance	Objective Evidence
Electrostatic discharge (ESD) IEC 60601-1-2 <ul style="list-style-type: none"> <li>EN 55024</li> <li>CISPR 24</li> <li>EN/IEC 61000-4-2</li> </ul>	± 2/4 kV indirect ± 2/4 kV direct ± 2/4/8 kV air	± 2/4 kV indirect ± 2/4 kV direct ± 2/4/8 kV air	Floors should be wood, concrete, or ceramic tile. If floors are covered with synthetic material, the relative humidity should be at least 30%.	NOTE 3
Electrical fast transient/burst (EFT) IEC 60601-1-2 <ul style="list-style-type: none"> <li>EN 55024</li> <li>CISPR 24</li> <li>EN/IEC 61000-4-4</li> </ul>	± 1 kV for power supply lines ±500V for input/output lines	± 1 kV for power supply lines ±500V for input/output lines	Mains power should be that of a typical commercial or hospital environment.	NOTE 3
Fast Transient Surge (FTS) IEC 60601-1-2 <ul style="list-style-type: none"> <li>EN 55024</li> <li>CISPR 24</li> <li>EN/IEC 61000-4-5</li> </ul>	± 500V/1 kV differential mode ± 2 kV common mode	± 500V/1 kV differential mode ± 2 kV common mode	Mains power should be that of a typical commercial or hospital environment.	NOTE 3
Voltage dips, short interruptions and voltage variations on power supply input lines IEC 60601-1-2 <ul style="list-style-type: none"> <li>EN 55024</li> <li>CISPR 24</li> <li>EN/IEC 61000-4-11</li> </ul>	<5% $U_t$ (>95% dip in $U_t$ ) for 0.5 cycles <40% $U_t$ (>60% dip in $U_t$ ) for 5 cycles <70% $U_t$ (>30% dip in $U_t$ ) for 25 cycles <5% $U_t$ (>95% dip in $U_t$ ) for 5 s	<5% $U_t$ (>95% dip in $U_t$ ) for 0.5 cycles <40% $U_t$ (>60% dip in $U_t$ ) for 5 cycles <70% $U_t$ (>30% dip in $U_t$ ) for 25 cycles <5% $U_t$ (>95% dip in $U_t$ ) for 5 s	Mains power should be that of a typical commercial or hospital environment. If the user requires continued operation during power mains interruptions, it is recommended that power be supplied from an applicably rated uninterruptible power supply or a battery.	NOTE 3

## Guidance and Manufacturer's Declaration–Electromagnetic Immunity (cont'd.)

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment – Guidance	Objective Evidence
Power frequency (50/60 Hz) magnetic field IEC 60601-1-2 <ul style="list-style-type: none"> <li>• EN 55024</li> <li>• CISPR 24</li> <li>• EN/IEC 61000-4-8</li> </ul>	3 A/m	3 A/m	Power frequency magnetic fields should be at levels characteristic of a typical location in a typical commercial or hospital environment.	NOTE 3
NOTE: $U_t$ is the a.c. mains voltage prior to application of the test level. NOTE 1: At 80 MHz and 800 MHz, the higher frequency range applies. NOTE 2: These guidelines may not apply in all situations. Electromagnetic propagation is affected by reflection from structures, objects, and people. NOTE 3: See TR09157.pdf (part of DOC0723504).				


## Guidance and Manufacturer's Declaration–Electromagnetic Immunity

The MUSE DL370 G6 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL370 G6 server should assure that it is used in such an environment.

## Guidance and Manufacturer's Declaration–Electromagnetic Immunity

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment – Guidance	Objective Evidence
Conducted RF IEC 60601-1-2 <ul style="list-style-type: none"> <li>• EN 55024</li> <li>• CISPR 24</li> <li>• EN/IEC 61000-4-6</li> </ul>	3 Vrms 150 KHz to 80 MHz @ 1 KHz mod.	V1 V rms	Portable and mobile RF communications equipment should be used no closer to any part of the [equipment or system], including cables, than the recommended separation distance calculated from the equation applicable to the frequency of the transmitter. Recommended separation distance $d = [3.5/V1]\sqrt{P}$	NOTE 3
Radiated RF IEC 60601-1-2 <ul style="list-style-type: none"> <li>• EN 55024</li> <li>• CISPR 24</li> <li>• EN/IEC 61000-4-3</li> </ul>	3 V/m 80 MHz to 1,000 MHz @ 1 KHz mod.	E1 V/m	$d = [3.5/E1]\sqrt{P}$ 80 MHz to 800 MHz $d = [7/E1]\sqrt{P}$ 800 MHz to 1.0 GHz	NOTE 3

## Guidance and Manufacturer's Declaration–Electromagnetic Immunity (cont'd.)

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment – Guidance	Objective Evidence
			<p>where <math>P</math> is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer and <math>d</math> is the recommended separation distance in meters (m). Field strengths from fixed RF transmitters, as determined by an electromagnetic site survey,<sup>a</sup> should be less than the compliance level in each frequency range.<sup>b</sup> Interference may occur in the vicinity of equipment marked with the following symbol:</p> 	
<p>NOTE 1: At 80 MHz and 800 MHz, the higher frequency range applies.</p> <p>NOTE 2: These guidelines may not apply in all situations. Electromagnetic propagation is affected by reflection from structures, objects, and people.</p> <p>NOTE 3: See TR09157.pdf (part of DOC0723504).</p>				
a	Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radio, AM and FM radio broadcast and TV broadcast cannot be predicted theoretically with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, an electromagnetic site survey should be considered. If the measured field strength in the location in which the MUSE DL370 G6 server is used exceeds the applicable RF compliance level above, the MUSE DL370 G6 server should be observed to verify normal operation. If abnormal performance is observed, additional measures may be necessary, such as re-orienting or relocating the MUSE DL370 G6 server.			
b	Over the frequency range 150 KHz to 80 MHz, field strengths should be less than 3 V/m.			

## Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL370 G6 Server

The MUSE DL370 G6 server is intended for use in the electromagnetic environment on which radiated RF disturbances are controlled. The customer or the user of the MUSE DL370 G6 server can help prevent electromagnetic interference by maintaining a minimum distance between portable and mobile RF communications equipment (transmitters) and the MUSE DL370 G6 server as recommended in the following table, according to the maximum output power of the communications equipment.



### Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL370 G6 Server

Rated Maximum Output Power of Transmitter W	Separation Distance (meters) According to Frequency of Transmitter		
	150 kHz to 80 MHz $d = 1.17\sqrt{P}$	80 MHz to 800 MHz $d = 1.17\sqrt{P}$	800 MHz to 1.0 GHz $d = 2.33\sqrt{P}$
0.01	0.12	0.12	0.23
0.1	0.37	0.37	0.74
1	1.17	1.17	2.33
10	3.7	3.7	7.3
100	11.7	11.7	23.3
<p>For transmitters rated at a maximum output power not listed above, the recommended separation distance <math>d</math> in meters (m) can be estimated using the equation applicable to the frequency of the transmitter, where <math>P</math> is the maximum output power rating of the transmitter in watts (w) according to the transmitter manufacturer.</p> <p>NOTE 1: At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies.</p> <p>NOTE 2: These guidelines may not apply in all instances. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people.</p>			

## EMC Exception(s) Disclosure

### EMC Exception(s) Disclosure

Type	Exception	Electromagnetic Environment Guidance
Electrostatic discharge (ESD)	None	N/A
Electrical fast transient/burst (EFT)	None	N/A
Fast Transient Surge (FTS)	None	N/A
Voltage dips, short interruptions and voltage variations on power supply input lines	None	N/A
Power frequency (50/60 Hz) magnetic field	None	N/A
Conducted RF	None	N/A
Radiated RF	None	N/A

# Electromagnetic Compatibility for ML370 G5 Server

The Muse ML370G5 fulfills the requirements of the following directives, standards, and normative documents:

- FCC 47CFR Part 15: Title 47–Telecommunication CHAPTER I–FEDERAL COMMUNICATIONS COMMISSION PART 15–RADIO FREQUENCY DEVICES
- Medical Devices Directive [MDD]: Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ No L 169/1 of 1993-07-12)

## Electromagnetic Compatibility Requirements (EMC)

### Electromagnetic Compatibility Requirements (EMC)

<p>EMC directive compliance used to support GEMS-IT information technology equipment (ITE) used in a medical device/system when the device:</p> <ul style="list-style-type: none"> <li>• Complies with applicable international EMC standards.</li> <li>• A risk analysis/assessment has determined the EMISSIONS and/or IMMUNITY of the ITE equipment shall not adversely affect the <b>essential performance</b> or <b>safety</b> of the SYSTEM.</li> <li>• The EMISSIONS of the ITE equipment shall not cause the EMISSIONS of the SYSTEM to exceed applicable limits.</li> </ul>	IEC 60601-1-2:2004	Medical electrical equipment – Part 1-2: General requirements for safety - Collateral standard: Electromagnetic compatibility - Requirements and tests
	• Per Annex HHH	Guidance for determining if non-medical electrical equipment used in a SYSTEM is exempt from the EMC testing requirements of this standard.
	EMC Directive: Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to Electromagnetic Compatibility (OJ L 139/19 of 1989-05-23)	
	EN 55022:1998 /A1:2000/A2:2003	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
	EN 55024:1998 /A1:2001/A2:2003	Information technology equipment - Immunity characteristics - Limits and methods of measurement
	EN 61000-3-2:2000	Electromagnetic compatibility (EMC) – Part 3-2: Limits - Limits for harmonic current emissions (equipment input current up to and including 16 A per phase)
	EN 61000-3-3:1995 /A1:2002	Electromagnetic compatibility (EMC) – Part 3-3: Limits; Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current less than or equal to 16 A per phase and not subject to conditional connection

**NOTE:**

The MUSE ML370G5 server is EN 55022, EN 55024, EN 61000-3-2, EN61000-3-3, and FCC compliant as declared by the OEM, HP. GE Healthcare installs additional components.

## Guidance and Manufacturer's Declaration—Electromagnetic Emissions

The MUSE DL360 G5 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL360 G5 should assure that it is used in such an environment.

### Guidance and Manufacturer's Declaration—Electromagnetic Emissions

Emissions Test	Compliance	Electromagnetic Environment—Guidance	Objective Evidence
RF emissions (Radiated) <ul style="list-style-type: none"> <li>30 MHz to 1,000 MHz IEC 60601-1-2:2004 CISPR22:1997 / A1:2000 / A2:2002 EN 55022:1998 / A1:2000 / A2:2003</li> <li>30 MHz to 5 GHz FCC 47CFR Part 15.33 FCC 47CFR Part 15.109</li> </ul>	Group 1 Class B	<b>Group 1 use</b> The MUSE ML370 G5 server uses RF energy only for its internal function. Therefore, its RF emissions are very low and are not likely to cause any interference in nearby electronic equipment.	NOTE 3
RF emissions (Conducted) <ul style="list-style-type: none"> <li>150 KHz to 30 MHz IEC 60601-1-2:2004 CISPR22:1997 / A1:2000 / A2:2002 EN 55022:1998 / A1:2000 / A2:2003</li> <li>150 KHz to 30 MHz FCC 47CFR Part 15.107</li> </ul>	Group 1 Class B	<b>Class B use</b> The MUSE ML370 G5 server is suitable for use in all establishments including domestic and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes.	NOTE 3

## Guidance and Manufacturer's Declaration—Electromagnetic Emissions (cont'd.)

Emissions Test	Compliance	Electromagnetic Environment—Guidance	Objective Evidence
Harmonic Emissions 2nd — 40th Harmonic IEC 60601-1-2:2004 EN 61000-3-2:2000 / A1:2001	Class A	<b>Class A</b> <ul style="list-style-type: none"> <li>Balanced three-phase equipment</li> <li>Household appliances, excluding equipment identified by Class D</li> <li>Tools excluding portable tools</li> <li>Dimmers for incandescent lamps</li> <li>Audio equipment</li> <li>Everything else that is not classified as B, C, or D</li> </ul> <b>Class B</b> Portable tools <ul style="list-style-type: none"> <li>Arc welding equipment that is not professional equipment</li> </ul> <b>Class C</b> <ul style="list-style-type: none"> <li>Lighting equipment</li> </ul> <b>Class D</b> (for power level 75W to 600W) <ul style="list-style-type: none"> <li>Personal computers and personal computer monitors</li> <li>Television receivers</li> </ul>	NOTE 3
Voltage fluctuations/ Flicker emissions IEC 60601-1-2:2004 EN 61000-3-3:1995 / A1:2002	Complies Pass		NOTE 3
NOTE 1: At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies. NOTE 2: These guidelines may not apply in all instances. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people. NOTE 3: See 2037193-017 MUSE HP ML370 EMC REPORT (DOC0343116).			

## Guidance and Manufacturer's Declaration—Electromagnetic Immunity

The MUSE DL360 G5 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL360 G5 server should assure that it is used in such an environment.

## Guidance and Manufacturer's Declaration—Electromagnetic Immunity

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment—Guidance	Objective Evidence
Electrostatic discharge (ESD) IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-2:1995 / A1:1998 / A2:2001</li> </ul>	± 2/4 kV indirect ± 2/4 kV direct ± 2/4/8 kV air	N/A ± 4 kV direct ± 8 kV air	Floors should be wood, concrete, or ceramic tile. If floors are covered with synthetic material, the relative humidity should be at least 30%.	NOTE 3
Electrical fast transient/burst (EFT) IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-4:1995 / A1:2001</li> </ul>	± 1 kV for power supply lines ±500V for input/output lines	± 1 kV for power supply lines ± 500V for input/output lines	Mains power should be that of a typical commercial or hospital environment.	NOTE 3
Fast Transient Surge (FTS) IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-5:1995 / A1:2001</li> </ul>	± 500V/1 kV differential mode ± 2 kV common mode	Power Lines: ± 1 kV differential ± 2 kV common mode I/O Lines: ± 500V differential ± 1 kV common mode	Mains power should be that of a typical commercial or hospital environment.	NOTE 3
Voltage dips, short interruptions, and voltage variations on power supply input lines IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-11:1994 / A1:2001</li> </ul>	<5% $U_t$ (>95% dip in $U_t$ ) for 0.5 cycles <40% $U_t$ (>60% dip in $U_t$ ) for 5 cycles <70% $U_t$ (>30% dip in $U_t$ ) for 25 cycles <5% $U_t$ (>95% dip in $U_t$ ) for 5 s	0% $U_t$ for 0.5 cycles N/A <70% $U_t$ (>30% dip in $U_t$ ) for 25 cycles 0% $U_t$ for 5 s	Mains power should be that of a typical commercial or hospital environment. If the user requires continued operation during power mains interruptions, it is recommended that power be supplied from an applicably rated uninterruptible power supply or a battery.	NOTE 3

## Guidance and Manufacturer's Declaration—Electromagnetic Immunity (cont'd.)

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment—Guidance	Objective Evidence
Power frequency (50/60 Hz) magnetic field IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-8:1993 / A1:2001</li> </ul>	N/A	N/A This device by its nature is not subject to the Power Frequency Immunity tests outlined in IEC/EN 61000-4-8: 1993 and CENELEC EN55024: 1998 +A1 +A2.	Power frequency magnetic fields should be at levels characteristics of a typical location in a typical commercial or hospital environment.	NOTE 3
NOTE: $U_t$ is the a.c. mains voltage prior to application of the test level. NOTE 1: At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies. NOTE 2: These guidelines may not apply in all instances. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people. NOTE 3: See 2037193-017 MUSE HP ML370 EMC REPORT (DOC0343116).				


## Guidance and Manufacturer's Declaration—Electromagnetic Immunity

The MUSE DL360 G5 server is intended for use in the electromagnetic environment specified in the following table. The customer or user of the MUSE DL360 G5 server should assure that it is used in such an environment.

## Guidance and Manufacturer's Declaration—Electromagnetic Immunity

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment—Guidance	Objective Evidence
Conducted RF IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-6:1996 / A1:2001</li> </ul>	3 Vrms 150 KHz to 80 MHz @ 1 KHz mod.	3 V rms	Portable and mobile RF communications equipment should be used on closer to any part of the [equipment or system], including cables, than the recommended separation distance calculated from the equation applicable to the frequency of the transmitter. <b>Recommended separation distance</b> $d = [3.5/3]\sqrt{P}$	NOTE 3

## Guidance and Manufacturer's Declaration—Electromagnetic Immunity (cont'd.)

Immunity Test	Compliance Test Level	Compliance Level	Electromagnetic Environment—Guidance	Objective Evidence
Radiated RF IEC 60601-1-2:2004 <ul style="list-style-type: none"> <li>EN 55024:1998 / A1:2001 / A2:2003</li> <li>EN 61000-4-3:2002 / A1:2002</li> </ul>	3 V/m 80 MHz to 1,000 MHz @ 1 KHz mod.	3 V/m	$d = [3.5/3]\sqrt{P}$ 80 MHz to 800 MHz $d = [7/3]\sqrt{P}$ 800 MHz to 1.0 GHz  where $P$ is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer and $d$ is the recommended separation distance in meters (m). Field strengths from fixed RF transmitters, as determined by an electromagnetic site survey, <sup>a</sup> should be less than the compliance level in each frequency range. <sup>b</sup> Interference may occur in the vicinity of equipment marked with the following symbol: 	NOTE 3
NOTE 1: At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies. NOTE 2: These guidelines may not apply in all instances. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people. NOTE 3: See 2037193-017 MUSE HP ML370 EMC REPORT (DOC0343116).				
a	Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radio, AM and FM radio broadcast and TV broadcast cannot be predicted theoretically with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, and electromagnetic site survey should be considered. If the measured field strength in the location in which the MUSE DL360 G5 is used exceeds the applicable RF compliance level above, the MUSE DL360 G5 should be observed to verify normal operation. If abnormal performance is observed, additional measures may be necessary, such as re-orienting or relocating the MUSE DL360 G5			
b	Over the frequency range 150 KHz to 80 MHz, field strengths should be less than 3 V/m.			

## Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL360 G5 Server

The MUSE DL360 G5 server is intended for use in the electromagnetic environment on which radiated RF disturbances are controlled. The customer or the user of the MUSE DL360 G5 server can help prevent electromagnetic interference by maintaining a minimum distance between portable and mobile RF communications equipment (transmitters) and the MUSE DL360 G5 server as recommended in the following table, according to the maximum output power of the communications equipment.

### Recommended Separation Distances Between Portable and Mobile RF Communications Equipment and the MUSE DL360 G5 Server

Rated Maximum Output Power of Transmitter $W$	Separation Distance (meters) According to Frequency of Transmitter		
	150 kHz to 80 MHz $d = 1.17\sqrt{P}$	80 MHz to 800 MHz $d = 1.17\sqrt{P}$	800 MHz to 1.0 GHz $d = 2.33\sqrt{P}$
0.01	0.12	0.12	0.23
0.1	0.37	0.37	0.74
1	1.17	1.17	2.33
10	3.70	3.70	7.37
100	11.7	11.7	23.3

For transmitters rated at a maximum output power not listed in this table, the recommended separation distance  $d$  in meters (m) can be estimated using the equation applicable to the frequency of the transmitter, where  $P$  is the maximum output power rating of the transmitter in watts (w) according to the transmitter manufacturer.

NOTE 1: At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies.

NOTE 2: These guidelines may not apply in all instances. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people.

## EMC Exception(s) Disclosure

### EMC Exception(s) Disclosure

Type	Exception	Electromagnetic Environment Guidance
Electrostatic discharge (ESD)	None	N/A
Electrical fast transient/burst (EFT)	None	N/A
Fast Transient Surge (FTS)	None	N/A
Voltage dips, short interruptions, and voltage variations on power supply input lines	None	N/A
Power frequency (50/60 Hz) magnetic field	None	N/A



## EMC Exception(s) Disclosure (cont'd.)

Type	Exception	Electromagnetic Environment Guidance
Conducted RF	None	N/A
Radiated RF	None	N/A





# National Health Service of Great Britain (NHS) Patient Identifiers

## Purpose

The National Health Service of Great Britain (NHS) requires applicable systems to comply to the national unique patient identifier schema specified in the **Information Standards Board for Health and Social Care** in **DSC Notice 32/2008 NHS Number Standard for Secondary Care (England)**.

Implementing the NHS number feature brings the MUSE system into compliance with these requirements

## Overview

The NHS assigns a 10-digit number to uniquely identify a person within the NHS domain. Systems that comply must validate and verify this number on input into the system and display the validation and verification status of the numbers. The number is validated using the modulus 11 algorithm, its tenth digit being the *checksum*. The number is verified in relation to the main NHS registry system to check existence and demographics correctness. It is also required that a compliant system display the NHS number in the 3 3 4 format on screen and on printed/exported output, that is, 123 456 7121 to enhance readability and to allow users to enter the Patient ID (PID) with or without spaces when searching for a patient or entering a new Patient ID.

For more information on installing the NHS number feature, see [“Installing the NHS Number Feature” on page 159](#) or [“Updating Legacy System Data ” on page 158](#).

## Number Validation

When the PID is inserted or modified in any patient test , the system runs the NHS Number validation algorithm. If the PID fails validation, the system displays the **Invalid PID** string in the mismatch display area of the MUSE Editor.

The check digit validation has five steps:

1. Multiply each of the first nine digits by a weighting factor as follows:

Position	Factor
1	10
2	9
3	8
4	7
5	6
6	5
7	4
8	3
9	2

2. Add the results of each multiplication together.
3. Divide the total by 11 and establish the remainder.
4. Subtract the remainder from 11 to give the check digit.
  - If the result is 11, then use a check digit of 0.
  - If the result is 10, then the NHS Number is invalid and not used.
5. Check that the remainder matches the check digit.  
If it does not match, the NHS Number is invalid.

## Number Verification

The MUSE system receives the PID verification status from the Hospital Information System (HIS) through the Inbound HL7 interface. The **PID** segment (Field 32, component 1) of ADT messages is used. The following table lists the valid numeric values for this field, along with their corresponding string enumeration:

### PID Verification Status Codes

Code	Description
01	Number present and verified
02	Number present but not traced
03	Trace required
04	Trace attempted - No match or multiple match found
05	Trace needs to be resolved - (NHS Number or patient detail conflict)
06	Trace in progress
07	Number not present and trace not required
08	Trace postponed (baby under six weeks old)

If the HIS does not provide the verification status with the ADT data, then the ADT data stored on the MUSE system for the patient is marked as **Number present and verified**. The MUSE system verifies the NHS Number (Patient ID) in tests using the following rules:

- If the site has **ADT Query** or **ADT Interface** enabled, and the ADT data is found for the Patient ID and no PID/Name mismatches exist, the Patient ID status is set to that of the ADT data.
- If the site has **ADT Query** or **ADT Interface** enabled, and the ADT data is found for the Patient ID and a PID/Name mismatch, the Patient ID is marked as **Trace needs to be resolved**.
- If the site has **ADT Query** or **ADT Interface** enabled, and ADT data is not found for the Patient ID, and the Patient ID is not a **NO PID**, **all nines**, or **all zeros**, then the Patient ID is marked as **present but not traced**.
- If the Patient ID is **NO PID** or **all nines**, that is 999999999, or **all zeros**, that is, 000000000, the Patient ID is marked as **Number not present**.
- When the test is set to **Demographics Complete**, the Patient ID verification status is marked as **verified**.

## Searching by Patient ID (PID)

The NHS number requirements specify that when users or other systems query the MUSE system for patient data by NHS number, the number need not be formatted in the 3 3 4 format, for example, 111 111 2222, 11 1111 222 2, or 1111112222. However, these values successfully return identical results for PID: 111 111 2222.

The design normalizes all user/system input regarding PID to the PID storage format. It was necessary to capture all points input into the system regarding PID, as follows:

- Editor
- Normalization
- HL7 Inbound Parser
- CSI Patient/Order queries
- DCP Patient/Order queries
- MUSE API Patient queries (servicing CASE, MUSE & CV Web)

### NOTE:

Database Search allows the user to input PID, but requires the user to enter the exact format, that is, 111 111 2222.

## Displaying the Patient ID

The NHS number requirements specify that the NHS number must be in the 3 3 4 format wherever displayed on the MUSE system.

The design for this, even though not optimal from a storage point of view, stores the NHS number in the 3 3 4 format, that is, 111 111 2222. The reasons for doing this are:

- Since the data is stored in the format in which it is displayed, no reformatting needs to be performed to display lists of test in the MUSE Editor, MUSE Web, ECG carts, CASE, MUSE Database Search, and MUSE Logs. Also, no reformatting is necessary

to display PIDs in data export formats, for example, postscript, PCL, PDF, XML, and so forth.

- The option to store the NHS numbers *spaceless* still requires data input normalization: normalizing PIDs to spaceless, plus additional code required to format PID at all of the points of export. With a large collection of data layers, this adds a great deal of complexity.
- It requires very slight optimization in displaying lists containing PIDs, since they do not need to be *post processed*.
- There is a precedence in the MUSE system to store Swedish and Danish PID formats that contain the — character (used as a separator) with the character in the database.

## Updating Legacy System Data

Since NHS may be added to an existing MUSE system that already contains patient data, a utility brings the current data into a consistent state required by the NHS number implementation. The utility sets the various PIDs in the proper format and adds a verification status.

1. Sets HIS Patient IDs to the correct format and sets verification status:
  - hisPatients.PatientID = <123 456 7890>
  - hisPatients.PID\_VerificationStatus = *Present and verified*.
2. Sets system Patient IDs to the correct format:
 

patPatients.PatientID = <123 456 7890>
3. Sets test Patient IDs to the correct format and sets the verification and validation status:
  - tstPatientDemographics.PatientID = <123 456 7890>
  - tstPatientDemographics.PID\_VerificationStatus = *Present and verified* (if test is democomplete or confirmed)
  - tstTests.InvalidPID = *true* (if PID is NHS invalid)
  - patPatients.PID\_VerificationStatus = *Present and verified* (if test is democomplete or confirmed)
4. Set Site configuration:
 

Set maximum PID length to a minimum of 12 characters.

Since updating the data is a potentially long running process, the following application was created to display the update status as the data is converted.

Domain	Type	Items	Completed	Status	Time
Ste0001	HIS Demographics	49968	49968	Done	00:13:38
	System Demographics	229031	229031	Done	01:01:04
	Tests - Confirmed	618603	143711		
	Tests - Unconfirmed	2947	0		
Ste0002	HIS Demographics	13902	0		
	System Demographics	46224	0		
	Tests - Confirmed	131366	0		
	Tests - Unconfirmed	6214	0		
Ste0003	HIS Demographics	0	0		
	System Demographics	44835	0		
	Tests - Confirmed	84397	0		
	Tests - Unconfirmed	1006	0		
Ste0032	HIS Demographics	0	0		
	System Demographics	0	0		
	Tests - Confirmed	0	0		
	Tests - Unconfirmed	0	0		
System	Site Configuration	4	0		

Progress: (34.4%) Cancel

Total Time: 01:52:11

## Installing the NHS Number Feature

To enable the NHS Number Feature, set: ***MUSE\_System.cfgSystem.CustomerID = CustomerID.NHSNumber (17)***.

The MUSE Installer allows you to update the ***CustomerID*** to the ***NHSNumber*** value.

## Modules and Files Affected

### assembly/MiddleTier/Common

Module Affected	Changes
Constants.cs	Added NHS Number verification status enumerations
DataMergeHelper.cs	Added NHS Number validation algorithm
FieldTags.cs	Added <i>PIDVerificationStatus</i> field enumeration for Patient Test support
FormatField.cs	Added NHS Number formatting methods
HISFieldTags.cs	Added <i>PIDVerificationStatus</i> field enumeration for HIS data support
SystemConfig.cs	Added <i>NHSNUMBER</i> enumeration to <i>CustomerID</i> .

### assembly/MiddleTier/Server/Common

Module Affected	Changes
ContextObject.cs	Update <i>PatientDemo</i> and <i>HISData</i> meta-data and containers to support NHS verification status

## assembly/MiddleTier/Server/HIS

Module Affected	Changes
HISDataLayer.cs	Update to include the NHS verification status enumeration for the <i>HISData</i> object
HISEvent.cs	Parse NHS verification status from incoming HL7 message
HISManager.cs	Update to normalize PID parameter used for filtering ADT list queries
HL7Provider.cs	Parse NHS verification status from incoming HL7 message

## assembly/MiddleTier/Server/Patient

Module Affected	Changes
ClientTestmanager.cs	Added merge of NHS verification status form HIS data to System demographics
Normalization.cs	Update to normalize PID coming into the system
PatientDemo.cs	Added <i>PIDVerificationStatus</i> field enumeration for System demographics data support
PatientTest.cs	Added trigger of NHS Number validation
PatientTestLists.cs	Update to normalized PID parameter used for filtering Patient and Test Retrieval list queries.

## assembly/MiddleTier/Triggers/TestCRUD

Module Affected	Changes
PatientDemoSync.cs	Updated to include merge of NHS verification status from test into system demographics

## assembly/MiddleTier/Triggers/TestFields

Module Affected	Changes
CommonTriggers.cs	Added trigger to calculate NHS Number status and updated trigger to normalize PID for test data
HISTriggers.cs	Added set field trigger to normalize PID for ADT data
Merge.cs	Added merge of NHS verification status from HIS data into test data

## assembly/UI/PatientDataForms

Module Affected	Changes
ADTPatientInfoForm.cs	Updated GUI to display NHS verification status
ADTPatientInfoForm.resx	
PatientInfoForm.cs	Updated GUI to display NHS verification status
PatientInfoForm.resx	



## database/update/07\_02\_00

Module Affected	Changes
Site.sql	Added support for PID verification status
System.sql	Added support for PID verification status

## include

Module Affected	Changes
syscalls.h	Added function signatures
sysinfo.h	Added function signatures

## library/museapi

Module Affected	Changes
museapi.c	Normalize PID to NHS format for museapi calls

## library/sys

Module Affected	Changes
gethisdb.cpp	Updated GetMacVUStyleOrderList to be NHS Number aware
getpatient.cpp	c data layer NHS Number formatting functions and normalize PID to NHS format for sys calls





# Glossary

archive	Permanent storage of data.
ACC	<b>American College of Cardiology.</b> A professional society whose membership comprises more than 24,000 cardiovascular physicians and scientists from around the world.
AIT	<b>Advanced Intelligent Tape.</b> A form of magnetic tape and drive using AME developed by Sony for storing large amounts of data. AIT features high speed file access, long head and media life, the ALDC compression algorithm, and a MIC chip.
ANSI	<b>American National Standards Institute.</b> The United States government body responsible for approving US standards in many areas, including computers and communications. ANSI is a member of ISO.
API	<b>Application Program Interface.</b> The interface (calling conventions) by which an application program accesses operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure the portability of the code.
ASCII	<b>American Standard Code for Information Interchange.</b> This is a standard means of representing characters, consisting of 256 characters. The first 128 characters are standardized, and the first 32 of those are control codes, which don't really represent visible characters but rather codes that can be used for text formatting or actions, such as making the computer beep. After the 32 control codes, the next 96 standardized characters represent numbers, letters (both uppercase and lowercase), and standard punctuation marks. The last 128 characters represent different things on different platforms.
ATAPI	<b>AT Attachment Packet Interface.</b> Part of the EIDE interface that provides additional commands to control a CD-ROM drive or magnetic tape.
backup	A spare copy of a file, file system or other resource for use in the event of failure or loss of the original.

BIOS	<b>Basic Input/Output System.</b> The part of the system software of the IBM PC and compatibles that provides the lowest level interface to peripheral devices and controls the first stage of the bootstrap process, including installing the operating system. The BIOS is stored in ROM, or equivalent, in every PC. Its main task is to load and execute the operating system which is usually stored on the computer's hard disk, but may be loaded from CD-ROM or floppy disk at install time.
BNC	<b>Bayonet Navy Connector.</b> A connector for coaxial cable such as that used for some video connections and RG58 "cheapernet" connections. A BNC connector has a bayonet-type shell with two small knobs on the female connector which lock into spiral slots in the male connector when it is twisted on.
cache	A small fast memory holding recently accessed data, designed to speed up subsequent access to the same data. Most often applied to processor-memory access but also used for a local copy of data accessible over a network etc.
CE Marking	<p>The European Commission refers to the CE Marking of products as a "passport" which can allow a manufacturer to freely circulate their products within the European marketplace. The marking applies only to products regulated by European health, safety and environmental protection legislation (product directives) but this is estimated to include more than 50% of the goods currently exported from the U.S. to Europe.</p> <p>The letters "CE" are an abbreviation of a French phrase "Conformite Europeene". The marking indicates that the manufacturer has conformed with all the obligations required by the legislation.</p>
client/server	A network system where a dedicated computer (server) handles some of the processing tasks while multiple smaller computers (clients) complete other processes by tapping into the server's shared files and programs.
CMOS	<b>Complementary Metal Oxide Semiconductor.</b> A semiconductor fabrication technology using a combination of n- and p-doped semiconductor material to achieve low power dissipation. Any path through a gate through which current can flow includes both n and p type transistors. Only one type is turned on in any stable state so there is no static power dissipation and current only flows when a gate switches in order to charge the parasitic capacitance.
CPU	<b>Central Processing Unit.</b> The part of a computer which controls all the other parts.
DICOM	<b>Digital Imaging and Communications in Medicine.</b> An industry standard to define connectivity and communication protocols of medical imaging devices. It conforms to the ISO reference model for network communications and incorporates object-oriented design concepts.
DIMM	<b>Dual In-line Memory Module.</b> Small circuit boards carrying memory integrated circuits, with signal and power pins on both sides of the board.

DLL	<p><b>Dynamically Linked Library.</b> A library which is linked to application programs when they are loaded or run rather than as the final phase of compilation. This means that the same block of library code can be shared between several tasks rather than each task containing copies of the routines it uses. The executable is compiled with a library of “stubs” which allow link errors to be detected at compile-time. Then, at run-time, either the system loader or the task's entry code must arrange for library calls to be patched with the addresses of the real shared library routines, possibly via a jump table.</p> <p>The alternative is to make library calls part of the operating system kernel and enter them via some kind of trap instruction. This is generally less efficient than an ordinary subroutine call.</p> <p>It is important to ensure that the version of a dynamically linked library is compatible with what the executable expects.</p>
DMA	<p><b>Direct Memory Access.</b> A facility of some architectures which allows a peripheral to read and write memory without intervention by the CPU. DMA is a limited form of bus mastering.</p>
DRAM	<p><b>Dynamic Random Access Memory.</b> A type of semiconductor memory in which the information is stored in capacitors on a MOS integrated circuit. Typically each bit is stored as an amount of electrical charge in a storage cell consisting of a capacitor and a transistor. Due to leakage the capacitor discharges gradually and the memory cell loses the information. Therefore, to preserve the information, the memory has to be refreshed periodically. Despite this inconvenience, the DRAM is a very popular memory technology because of its high density and consequent low price.</p>
DTMF	<p><b>Dual Tone Multi Frequency.</b> (“Touch-Tone”) A method used by the telephone system to communicate the keys pressed when dialling. Pressing a key on the phone's keypad generates two simultaneous tones, one for the row and one for the column. These are decoded by the exchange to determine which key was pressed.</p>
ECC	<p><b>Error Detection and Correction.</b> A collection of methods to detect errors in transmitted or stored data and to correct them. This is done in many ways, all of them involving some form of coding. The simplest form of error detection is a single added parity bit or a cyclic redundancy check. Multiple parity bits can not only detect that an error has occurred, but also which bits have been inverted, and should therefore be re-inverted to restore the original data. The more extra bits are added, the greater the chance that multiple errors will be detectable and correctable.</p>
ESD	<p><b>Electrostatic Discharge.</b> One kind of test that hardware usually has to pass to prove it is suitable for sale and use. The hardware must still work after it has been subjected to some level of electrostatic discharge. Some organizations have their own ESD requirements which hardware must meet before it will be considered for purchase. Different countries have different legal regulations about levels of ESD.</p>
Ethernet	<p>A popular method for sending data through a local area network using single channel cable and a special data collision protocol to detect network availability.</p>
expansion slot	<p>A connector in a computer into which an expansion card can be plugged. The connector supplies power to the card and connects it to the data bus, address bus and control signals of the motherboard.</p>

fax	<b>Facsimile.</b> A process by which fixed graphic material including pictures, text, or images is scanned and the information converted into electrical signals which are transmitted via telephone to produce a paper copy of the graphics on the receiving fax machine.
FAT	<b>File Allocation Table.</b> The component of an MS-DOS or Windows 95 file system which describes the files, directories and free space on a hard disk or floppy disk.
file server	A computer dedicated to managing the flow of information among networked computers and used as a storage location for programs and files shared by network users.
firmware	Refers to the software that is embedded onto a piece of hardware to control that hardware. Generally, firmware can be upgraded and is placed on an EEPROM. Sometimes, if a new driver for a piece of hardware is released, new firmware will also be released that is required to get the full functionality or performance of the driver. In other cases, firmware will have some bugs or undesirable features, and can be upgraded to work out the problems. Of course, the rest of the hardware cannot be upgraded without replacing pieces of it, so manufacturers try to store as many critical function controls as they can in the firmware, in case they need to change them. For them, it is the difference between recalling a product and simply telling their customers to upgrade the firmware.
FTP	<b>File Transfer Protocol.</b> The method of moving files from system to system using TCP/IP.
FTS	<b>Fast Transient Surge.</b>
gateway	A term for a device that enables data to flow between different networks (forming an internet).
HIS	<b>Hospital Information System.</b> A system that provides the information management features hospitals need for daily business. Typically includes patient tracking, billing and administrative programs. May also include clinical features.
HL7	<b>Health Level 7.</b> A standard interface for exchanging and translating data between computer systems.
Hot-pluggable	This type of mechanism implies that you can remove or add things while the system is running. For example, hard drives and power supplies are often candidates for this term. Normally, they come in special proprietary form factors in server machines and RAID boxes. If you've got mission-critical applications you want your servers to have as many hot swappable components as possible. Recently, servers have been introduced with hot-swappable PCI cards and buses.
IDE	<b>Integrated Drive Electronics.</b> A disk drive interface standard based on the IBM PC ISA 16-bit bus but also used on other personal computers.
IEC	<b>International Electrotechnical Commission.</b> The international standards and conformity assessment body for all fields of electrotechnology.

IEEE	<b>Institute of Electrical and Electronics Engineers, Inc.</b> The world's largest technical professional society, based in the USA. Founded in 1884 by a handful of practitioners of the new electrical engineering discipline, today's Institute has more than 320,000 members who participate in its activities in 147 countries. The IEEE sponsors technical conferences, symposia and local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics and computer engineering and computer science, provides educational programs for its members and promotes standardization. Areas covered include aerospace, computers and communications, biomedical technology, electric power and consumer electronics.
IIS	<b>Internet Information Server.</b> The name for Microsoft's webserver. It works with server versions of Microsoft's operations systems and was first developed for Windows NT Server.
I/O	<b>Input/Output.</b> Communication between a computer and its users, its storage devices, other computers (via a network) or the outside world. The devices the computer uses to do this are called "peripherals".
IrDA	<b>Infrared Data Association.</b> A non-profit trade association providing standards to ensure the quality and interoperability of infrared (IR) hardware. The association currently has a membership of over 160 companies from around the world, representing computer and telecommunications hardware, software, components and adapters.
IP	<b>Internet Protocol.</b> The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IRQ	<b>Interrupt Request.</b> The name of an input found on many processors which causes the processor to suspend normal instruction execution temporarily and to start executing an interrupt handler routine.
ISA	<b>Industry Standard Architecture.</b> A bus standard for IBM compatibles that extends the XT bus architecture to 16 bits.
ISO	<b>International Organization for Standardization.</b> A voluntary, nontreaty organization founded in 1946, responsible for creating international standards in many areas, including computers and communications. Its members are the national standards organizations of 89 countries, including the American National Standards Institute.
KVM Switch	<b>Keyboard Video Mouse switch.</b> This is a switch that connects 2 or more computers to the same keyboard, mouse, and monitor. The KVM switch fools each computer into thinking that they are actively connected to a separate keyboard, mouse and monitor. There is always some mechanism (a button and or keyboard command) on a KVM switch to switch between which computer accepts the input of the keyboard and mouse, and displays output to the monitor. Thus, when you move the mouse connected to the switch, your mouse movement is only echoed to the active computer at the time.
LAN	<b>Local Area Network.</b> A data communications network which is geographically limited (typically to a 1 km radius) allowing easy interconnection of terminals, microprocessors and computers within adjacent buildings.

LCD	<b>Liquid Crystal Display.</b> An electro-optical device used to display digits, characters or images, commonly used in digital watches, calculators, and portable computers.
LED	<b>Light-Emitting Diode.</b> A type of diode that emits light when current passes through it.
MIME	<b>Multipurpose Internet Mail Extensions.</b> Refers to functions used for the attachment of binary files to an e-mail message. MIME is the most common group of functions used to make this translation, and allows us to tack on graphics, sound, and executable files to our e-mail messages.
motherboard	The main printed circuit board in an electronic device, particularly a computer, which may contain sockets that accept additional boards ("daughter-boards"). In a personal computer, the motherboard contains the bus, the microprocessor, and integrated circuits used for controlling any built-in peripherals such as the keyboard, text and graphics display, serial ports and parallel ports, and mouse interfaces.
MPEG	<b>Moving Picture Experts Group.</b> An ISO committee that generates standards for digital video compression and audio. Also the name of their algorithms.
NEMA	<b>National Electrical Manufacturers Association.</b>
NetBIOS	<b>Network Basic Input/Output System.</b> An applications programming interface (API) which activates network operations on IBM PC compatibles running under Microsoft's DOS. It is a set of network commands that the application program issues in order to transmit and receive data to another host on the network. The commands are interpreted by a network control program or network operating system that is NetBIOS compatible.
NetBEUI	<b>NetBIOS Extended User Interface.</b> The network transport protocol used by all of Microsoft's network systems and IBM's LAN Server based systems.
NIC	<b>Network Interface Card.</b> An adapter circuit board installed in a computer to provide a physical connection to a network.
ns	<b>nanosecond.</b> 10 <sup>-9</sup> seconds (one thousand millionth part of a second)
OEM	<b>Original Equipment Manufacturer.</b> A company which makes equipment (e.g. computers) as opposed to one which sells equipment made by other companies.
OS	<b>Operating System.</b> The program that allows you to access the basic functions of your computer. It is the minimum software required to run a program.
PBX	Private Branch Exchange. A telephone exchange local to a particular organization who use, rather than provide, telephone services. The earliest PBXs were manual (Private Manual Branch EXchange, PMBX) but are now more likely to be automatic (Private Automatic Branch eXchange).
PCB	<b>Printed Circuit Board.</b> A thin board to which electronic components are fixed by solder. Component leads and integrated circuit pins may pass through holes ("vias") in the board or they may be surface mounted, in which case no holes are required (though they may still be used to connect different layers).



PCI	<b>Peripheral Component Interconnect.</b> A standard for connecting peripherals to a personal computer.
PCL	<b>Printer Control Language.</b> A Document description language used by Hewlett-Packard LaserJet printers.
PDC	<b>Primary Domain Controller.</b> In Windows NT, this machine is the main machine that responds to security authentication requests, such as logging in, within its domain. The PDC may be backed by one or more backup domain controllers that can also handle security authentication.
PDF	<b>Portable Document Format.</b> The native file format for Adobe Systems' Acrobat. PDF is the file format for representing documents in a manner that is independent of the original application software, hardware, and operating system used to create those documents.
PING	<b>Packet Internet Groper.</b> A program used to test reachability of destinations by sending them one, or repeated, ICMP echo requests and waiting for replies.
PostScript	A Page Description Language based on work originally done by John Gaffney at Evans and Sutherland in 1976, evolving through "JaM" ("John and Martin", Martin Newell) at XEROX PARC, and finally implemented in its current form by John Warnock et al. after he and Chuck Geschke founded Adobe Systems, Inc. in 1982. Its primary application is to describe the appearance of text, graphical shapes and sampled images on printed or displayed pages.
PRML	<b>Partial Response Maximum Likelihood.</b> A method for converting the weak analog signal from the head of a magnetic disk drive into a digital signal. PRML attempts to correctly interpret even small changes in the analog signal, whereas peak detection relies on fixed thresholds. Because PRML can correctly decode a weaker signal it allows higher density recording.
PS/2	IBM's second generation of personal computers. The PS/2 series introduced three advances over the PC series: 3.5" 1.44 megabyte microfloppy disks, VGA and 8514 graphics display standards, and the Micro Channel bus architecture. The 3.5" disks and VGA can be easily installed on other PCs and will become the standard for new compatible computers.
RAID	<b>Redundant Array of Inexpensive Disks/Drives.</b> A unit with several magnetic disks which protects against data loss in the event of the failure of any one disk.
RAM	<b>Random Access Memory.</b> A data storage device for which the order of access to different locations does not affect the speed of access.
RFI	<b>Radio Frequency Interference.</b> Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of their normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits.
RISC	<b>Reduced Instruction Set Computer.</b> A processor whose design is based on the rapid execution of a sequence of simple instructions rather than on the provision of a large variety of complex instructions.
RJ-45	A serial connector which looks very much like a standard telephone connector, except it houses eight wires instead of four.

ROM	<b>Read-Only Memory.</b> A type of data storage device which is manufactured with fixed contents. In its most general sense, the term might be used for any storage system whose contents cannot be altered. The term is most often applied to semiconductor integrated circuit memories, of which there are several types, and CD-ROM.
RS-232	The most common asynchronous serial line standard.
SCSI	<b>Small Computer System Interface.</b> A processor-independent standard for system-level interfacing between a computer and intelligent devices including hard disks, floppy disks, CD-ROM, printers, scanners, and many more.
seek time	The time it takes for a disk drive to move its head(s) from one track to another. The seek time depends on the power of the servo, the mass of the heads, the number of tracks traversed and the time taken to position the heads over the target track accurately enough to start data transfer.
SIMM	<b>Single In-line Memory Module.</b> A small circuit board or substrate, typically about 10cm x 2cm, with RAM integrated circuits or die on one or both sides and a single row of pins along one long edge. Several SIMMs are mounted with their substrates at right-angles to the main circuit board (the motherboard). This configuration allows greater packing density than direct mounting of, e.g. DIL (dual in-line) RAM packages on the motherboard. In 1993 one SIMM typically held one or four megabytes, by early 1997 one could hold 8, 16, or 32 MB.
SMTP	<b>Simple Mail Transfer Protocol.</b> A protocol defined in STD 10, RFC 821, used to transfer electronic mail between computers, usually over Ethernet. It is a server to server protocol, so other protocols are used to access the messages.
STS	<b>Society for Thoracic Surgeons.</b>
Subnet Mask	This is a TCP/IP number used to determine which TCP/IP subnet a device belongs to. Devices in the same subnet can be communicated with locally without going through a router. When a TCP/IP device tries to communicate with another device, the bits of the TCP/IP destination address are "ANDed" with the subnet mask to determine whether the address is a local address (broadcastable) or must be reached through a router.
TCP/IP	<b>Transmission Control Protocol over Internet Protocol.</b> The de facto standard Ethernet protocols incorporated into 4.2BSD Unix. TCP/IP was developed for internetworking and encompasses both network layer and transport layer protocols.
tack ball	A pointing device consisting of a ball housed in a socket containing sensors to detect rotation of the ball about two axes - like an upside-down mouse. The user rolls the ball with his thumb or the palm of his hand to move a cursor. Track balls are common on modern portable computers, where there may be no desk space on which to use a mouse. Some clip onto the side of the keyboard and have integral buttons which have the same function as mouse buttons.
twisted pair	A type of cable in which pairs of conductors are twisted together to randomize possible cross-talk from nearby wiring. Inadequate twisting is detectable using modern cable testing instruments.
UDMA	<b>Ultra Direct Memory Access.</b> A development of the Advanced Technology Attachment specifications which gives nearly twice the maximum transfer speed of the ATA-3 standard (PIO Mode 4).

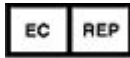
UL	<b>Underwriters Laboratories Inc.</b> is an independent, not-for-profit product safety testing and certification organization.
UNC	<b>Universal Naming Convention.</b> The name given for the naming used when one specifies: \\the sever\the volume\the path\then the file name of a file. An example of a UNC is: \\Myserver\Docdrive\Magazine\glossary.doc
UPS	<b>Uninterruptible Power Supply.</b> Unit which supplies ten minutes of battery backup power to the file server in the event of main power source failure.
USB	<b>Universal Serial Bus.</b> A technology in the works that will replace the current way that some peripheral devices connect to your computer. It is much faster than serial and parallel communications. It is also much more flexible: it will be able to connect to possibly hundreds of devices simultaneously.
VESA	<b>Video Electronics Standards Association.</b> An industry standards organization created in 1989/1990 primarily concerned with IBM compatible personal computers. The first standard it created was the 800 x 600 pixel Super VGA (SVGA) display and its software interface. It also defined the VESA Local Bus (VLB).
VGA	<b>Video Graphics Array.</b> A display standard for IBM PCs, with 640 x 480 pixels in 16 colors and a 4:3 aspect ratio. There is also a text mode with 720 x 400 pixels.







GE Medical Systems  
*Information Technologies, Inc.*  
8200 West Tower Avenue  
Milwaukee, WI 53223 USA  
Tel: +1 414 355 5000  
+1 800 558 7044 (US Only)  
Fax: +1 414 355 3790



GE Medical Systems  
*Information Technologies GmbH*  
Munzinger Straße 5  
D-79111 Freiburg Germany  
Tel: +49 761 45 43 -0  
Fax: +49 761 45 43 -233

## Asia Headquarters

GE Medical Systems  
*Information Technologies, Inc.*  
Asia; GE (China) Co., Ltd.  
1 Huatuo Road  
Zhangjiang Hi-tech Park Pudong  
Shanghai, People's Republic of China 201203  
Tel: +86 21 3877 7888  
Fax: +86 21 3877 7451

GE Medical Systems *Information Technologies, Inc.*, a General Electric Company, going to market as GE Healthcare.

[www.gehealthcare.com](http://www.gehealthcare.com)

