

GE Healthcare

# MUSE™ v9

## Cardiology Information System

### Service Manual

Software Version 9  
2059568-017 Revision D



MUSE v9 Cardiology Information System  
English  
© 2015-2017 General Electric Company.  
All Rights Reserved.

## Publication Information

The information in this document applies only to MUSE™v9 Cardiology Information System. It does not apply to earlier product versions. Due to continuing product innovation, specifications in this document 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	Comments
A	1 May 2015	Initial release.
B	17 July 2015	Customer release.
C	7 December 2016	Updated to support HCSDM00417312, HCSDM00430822, and HCSDM00426008.
D	7 September 2016	Updated to support HCSDM00432551 for LDAP/AD authentication.

To access other GE Healthcare Diagnostic Cardiology documents, 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) documents, go to the device manufacturer's website.

This document describes the MUSE Cardiology Information System, also referred to as the "product", "system", or "device". This document 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.

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.

This document provides information required for the proper use of the system. Familiarize yourself with this information, and read and understand all instructions before attempting to use this system. Keep this document with the equipment at all times and periodically review it.

### NOTE:

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

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

## Service Manual Language Information

WARNING (EN)	This service manual is available in English only. <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)	Това упътване за работа е налично само на английски език. <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>

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

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>
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 tekniker, 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>

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

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>
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 (EL)	<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>

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

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, stjórnanda eða sjúklingi frá raflösti, vélrænum eða öðrum áhættum.</li> </ul>
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 kejutan 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>
CẢNH BÁO (VI)	<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>

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

ECKEPTU (KK)	<p>Бұл қызмет көрсету бойынша нұсқаулығы тек ағылшын тілінде қолжетімді.</p> <ul style="list-style-type: none"> <li>Тұтынушының қызмет провайдері ағылшын тілінен басқа тілдегі нұсқаны талап етсе, аудару бойынша қызметтерімен қамтамасыз ету тұтынушы жауапкершілігінде болуы тиіс.</li> <li>Бұл қызмет көрсету бойынша нұсқаулығын назарға алып, түсінбегенше, жабдыққа қызмет көрсетуден бас тартыңыз.</li> <li>Бұл ескертуді елемей қызмет провайдері, оператор немесе емделушінің электр шоғынан, механикалық немесе басқа қауіптер нәтижесінде жарақат алуына әкелуі мүмкін.</li> </ul>
BRĪDINĀJUMS (LV)	<p>Šī apkopotāju rokasgrāmata ir pieejama tikai anglu valodā.</p> <ul style="list-style-type: none"> <li>Ja apkalošanas sniedzējam nepieciešama informācija citā, nevis anglu, 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>
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>

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

<p>AVISO (PT-PT)</p>	<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 noutra linguagem, 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>
<p>AVERTISMENT (RO)</p>	<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 depănatorului, operatorului sau pacientului în urma pericolelor de electrocutare, mecanice sau de altă natură.</li> </ul>
<p>ПРЕДУПРЕЖДЕНИЕ (RU)</p>	<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>
<p>UPOZORENJE (SR)</p>	<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>
<p>VAROVANIE (SK)</p>	<p>Tento návod na obsluhu je k dispozícii len v angličtine.</p> <ul style="list-style-type: none"> <li>• Ak zákazníkovi 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>
<p>OPOZORILO (SL)</p>	<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>

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

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>
ЗАСТЕРЕЖЕННЯ (UK)	<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>
CẢNH BÁO (VI)	<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

<b>1</b>	<b>Product Overview</b>	
	Related Documents.....	13
	Safety Conventions .....	14
	Safety Hazards .....	14
	Hardware Specifications .....	15
	Software Specifications.....	15
	SQL Server Requirements.....	16
	Required Network Ports .....	16
	Antivirus Software.....	16
	Security Updates.....	16
	Installation Media .....	17
	MUSE Options.....	17
	MUSE Services .....	20
	MUSE v9 Drive Contents and Supporting Folders .....	22
	MUSE Application with Local Database .....	22
	MUSE Application with Remote Database .....	23
<b>2</b>	<b>System Setup</b>	
	Configuring Windows High Contrast Color Scheme on MUSE Client.....	26
	Changing the Default Rhythm Lead(s) in ECG Format Settings.....	26
	setlead1.bat Tool .....	27
	setlead3.bat Tool .....	28
	MUSE Report Distribution Configuration Report (DumpReportDist.bat).....	28
	Import and Export Profiles Tool.....	29
	Launching the Import and Export Profiles Tool .....	29
	Exporting a Profile.....	30
	Importing a Profile.....	30

<b>Changing the MUSE CSI Order Download Filtering and Sizing .....</b>	<b>30</b>
Limiting CSI MUSE Order Downloads by Test Type .....	30
Increasing or Decreasing the Number of CSI Order Downloads .....	32
<b>Stress List Management.....</b>	<b>34</b>
New String for Stress Tests .....	35
Creating a Worksheet .....	35
Retiring Strings.....	38
Unretiring Strings.....	38
Changing the Sort Order of Strings.....	38
Combining Unretire and Changing Sort Order Queries.....	39
Correcting Mistakes.....	39

### **3 MUSE Service Users**

<b>MUSE Service User Accounts.....</b>	<b>41</b>
MUSE User Accounts.....	41
Windows User Accounts .....	42
SQL Server Role Requirements.....	43
MUSE InstallShield Wizard Requirements.....	43
<b>Changing MUSE Service Accounts.....</b>	<b>44</b>
Changing the MUSE Service Account Passwords in the MUSE System.....	44
Changing the MUSE Service Accounts and Passwords in Windows .....	45
<b>Configuring SQL Server Security .....</b>	<b>47</b>
MUSE Background User Access Information .....	47
Create a SQL Server Login .....	48
Assign SQL Server Roles to a Login.....	48
Create SQL Server Database Users and Assign Roles .....	49

### **4 Application Authentication**

<b>MUSE Authentication .....</b>	<b>51</b>
Description .....	51
Enabling and Disabling MUSE Authentication.....	51
<b>Windows Authentication.....</b>	<b>52</b>
Description .....	52
Enabling and Disabling Windows Authentication .....	52
Mapping MUSE User Account to a Windows User Account for Windows Authentication .....	52
<b>LDAP Authentication .....</b>	<b>53</b>
Description .....	53
Enabling and Disabling LDAP Authentication .....	53
<b>Windows + LDAP Authentication .....</b>	<b>54</b>
<b>MUSE Shortcuts.....</b>	<b>54</b>
Using MUSE InstallShield Wizard to Create MUSE Shortcuts .....	54
Manually Modifying MUSE Shortcuts .....	55

### **5 System Administration**

<b>Auto Shutdown.....</b>	<b>57</b>
Activating System Auto Shutdown .....	58
Canceling the System Shutdown .....	59

	<b>Modifying the MUSE Installed Configuration .....</b>	<b>59</b>
	<b>Moving the MUSE Databases .....</b>	<b>60</b>
	<b>Renaming the MUSE Systems.....</b>	<b>65</b>
	Renaming the MUSE Application Server.....	65
	Renaming the MUSE HL7 Interface (CCG Server) .....	70
	Renaming the MUSE Client .....	70
	.....	70
	<b>Changing the MUSE Port Number .....</b>	<b>70</b>
<b>6</b>	<b>Maintenance</b>	
	<b>OEM Maintenance .....</b>	<b>73</b>
	<b>Safe Shutdown Procedures .....</b>	<b>73</b>
	Shutting Down the MUSE Application Server.....	73
	Shutting Down the MUSE Remote Database Server .....	74
	Shutting Down the MUSE HL7 Interface (CCG) .....	74
	Shutting Down the MUSE Client.....	74
	<b>Functional Checkout Procedures .....</b>	<b>74</b>
	Hardware FRU Repairs .....	74
	Non-FRU Repairs .....	75
	Optional Hardware Accessories for MUSE .....	79
<b>7</b>	<b>Disaster Recovery</b>	
	<b>MUSE System Backup and Recovery .....</b>	<b>81</b>
	Windows Operating System and SQL Server.....	81
	MUSE System Software.....	81
	MUSE Database Backup .....	82
	MUSE Database Restoration .....	82
	MUSE Application Server Disaster Recovery.....	83
	<b>MUSE HL7 Interface (CCG) Backup and Recovery .....</b>	<b>83</b>
	MUSE HL7 Interface (CCG) Configuration Backup and Restoration.....	83
	MUSE HL7 Interface (CCG) Disaster Recovery .....	84
	<b>MUSE Test System Disaster Recovery .....</b>	<b>84</b>
	<b>MUSE Client Disaster Recovery .....</b>	<b>84</b>
<b>A</b>	<b>National Health Service of Great Britain (NHS) Patient Identifiers</b>	
	<b>Overview .....</b>	<b>85</b>
	<b>Number Validation .....</b>	<b>85</b>
	<b>Number Verification .....</b>	<b>86</b>
	<b>Searching by Patient ID (PID).....</b>	<b>87</b>

	<b>Displaying the Patient ID .....</b>	<b>87</b>
	<b>Installing the NHS Number Feature .....</b>	<b>88</b>
	Enable NHS Number during Initial MUSE Database Installation .....	88
	Enable NHS Number by Manually Changing the Customer ID of the System .....	88
	<b>Updating Legacy System Data .....</b>	<b>88</b>
	Utility .....	88
	Application .....	89
<b>B</b>	<b>MUSE Database Language Change Tool</b>	
	<b>Installing the Database Language Change Tool .....</b>	<b>91</b>
	<b>Running the Database Language Change Tool .....</b>	<b>91</b>
	<b>Verifying the Database Language Change .....</b>	<b>92</b>
<b>C</b>	<b>Configuring MUSE System for LDAP Authentication</b>	
	<b>Installing the LDAP Authentication Option in the MUSE System .....</b>	<b>94</b>
	<b>Configuring LDAP in the MUSE System .....</b>	<b>95</b>
	1. Configuring LDAP in the MUSE System Properties .....	95
	2. Configuring LDAP Fields in MUSE Setup .....	97
	3. Configuring LDAP Groups in MUSE Setup .....	98
	<b>Changes to LDAP Groups .....</b>	<b>99</b>
	<b>ADSI Edit .....</b>	<b>100</b>
	Installing ADSI Edit .....	100
	Using ADSI Edit .....	100
<b>D</b>	<b>Support for MARS Holter Reports on MUSE v9 Systems Using Simplified Chinese Language Option</b>	
	<b>.....</b>	<b>103</b>
<b>E</b>	<b>Retrieving MUSE Error Logs on the SQL Server Management Studio</b>	
	<b>.....</b>	<b>107</b>
<b>F</b>	<b>Holter Recreate Tool</b>	
	<b>.....</b>	<b>109</b>
<b>G</b>	<b>Glossary</b>	
	<b>.....</b>	<b>111</b>

# Product Overview

The MUSE 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 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 system can be connected to non-GE Healthcare equipment if the equipment is recommended by GE Healthcare and meets the appropriate criteria.

This software system stores ECGs generated by a computerized analysis program that is used to interpret ECG tracings. This computerized interpretation is only significant when used in conjunction with clinical findings.

This chapter provides a general description of the MUSE v9 system, a list of other documents that support the product, its services, drive contents, and supporting folders.

## Related Documents

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

Part Number	Document Title
2059568-011	MUSE v9 Cardiology Information System Installation and Upgrade Manual
2059568-012	MUSE v9 Cardiology Information System Client Installation Manual
2059568-018	MUSE v9 Cardiology Information System Pre-Installation Manual
2059568-019	MUSE v9 Cardiology Information System Advanced Security Guide
2059568-009	MUSE v9 Cardiology Information System Operator Manual
2059568-013	MUSE v9 Cardiology Information System Devices and Interfaces Manual
2059568-025	MUSE v9 Cardiology Information System Transactional XML Developer's Manual
2059568-010	MUSE v9 Cardiology Information System Interval Editor User Guide
2020299-021	MobileLink Installation Manual

Part Number	Document Title
2059568-016	MUSE v9 Cardiology Information System Regulatory and Safety Manual
2020299-025	LAN Option for MAC Installation and Troubleshooting
2059568-020	CCG Installation Manual
2059568-021	MUSE v9 Cardiology Information System HL7 Interface Reference Manual
2059568-023	MUSE DICOM Gateway Pro Conformance Statement
2059868-024	CCG MPI Installation Manual
2020375-041	MUSE FDA XML Conversion 5D.02+
2046472-001	MultiTech Modem Driver Installation Instruction
2059868-026	MUSE InSite ExC Installation Manual
2107900-001	CV Web 3.0 Operator Manual
2107900-002	CV Web 3.0 Pre-Installation Manual
2107900-003	CV Web 3.0 Installation Manual
2107900-004	MUSE Enterprise Integration Reference Manual
2107900-005	MUSE Enterprise Integration Component Manual

## 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 safety messages alert you to potentially hazardous conditions that could arise during the normal use of this product and recommend steps that can be taken to avoid those conditions. Safety messages pertaining to hazardous conditions

that may arise during specific actions may also be provided during the discussion of those actions in this or other manuals for this product.

**CAUTION:**

DATA 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.

**CAUTION:**

DATA 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.

**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.

**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.

**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 AutoShutdown feature to notify users of the shutdown.

## Hardware Specifications

For hardware requirements, refer to the *MUSE v9 Cardiology Information System Pre-Installation Manual*.

## Software Specifications

For information regarding software requirements and specifications, refer to the *MUSE v9 Cardiology Information System Pre-Installation Manual*.

## SQL Server Requirements

For information regarding SQL Server requirements, refer to the *MUSE v9 Cardiology Information System Pre-Installation Manual*.

## Required Network Ports

For information regarding networking requirements for the MUSE system, refer to “Required Network Ports” in the *MUSE v9 Cardiology Information System Pre-Installation Manual*.

## Antivirus Software

Customers are advised to use antivirus protection. Virus protection software is not included with the system. GE Healthcare has tested the system with Norton Antivirus and McAfee Antivirus products. Antivirus products from other vendors can be used as long as they are qualified for the operating system on which they are being used.

Antivirus (AV) software is the responsibility of the customer. Due to the large number of antivirus applications on the market and their continual upgrade and version changes, GE Healthcare cannot guarantee full compatibility with all versions.

The following list provides antivirus exception information related to the MUSE system:

- Real-time antivirus scanning should be disabled during the installation or upgrade of a MUSE application server.
- Real-time antivirus scanning should be disabled during the installation or upgrade of a MUSE client workstation.
- Real-time antivirus scanning should be disabled during the installation of CCG software.
- Real-time antivirus scanning should exclude the **\\gehc-it** folder and all subfolders on systems where CCG software is installed.

In addition to the above, GE Healthcare reserves the right to request:

- Software exceptions for the system and its associated services.
- Real-time scanning exclusion of certain folders or files.
- Temporary disabling of antivirus software during installation or troubleshooting of the system.

## Security Updates

The GE Healthcare Product Security Database website lists the patches available by product to address system security.

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, use the following procedure:

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 Website to identify security patches that you can apply to your system.

## Installation Media

The core software included with the system is on two DVDs.

These DVDs contain both the content and ISOs of the content. The DVD can be used to directly access the content, or the ISOs can be used by service or the customer for mounting the media in a virtual environment to access the content. The following tables describe the content of the core software DVDs. Any other discs included with the MUSE system only contain content and do not contain ISOs.

### MUSE Application and Support DVD

Type	Name	Description
Folder	\MUSE9_Application	MUSE 9 application files
Folder	\MUSE9_Support	MUSE 9 support files
File	\MUSE9_Application.iso	ISO of the MUSE 9 application files
File	\MUSE9_Support.iso	ISO of the MUSE 9 support files

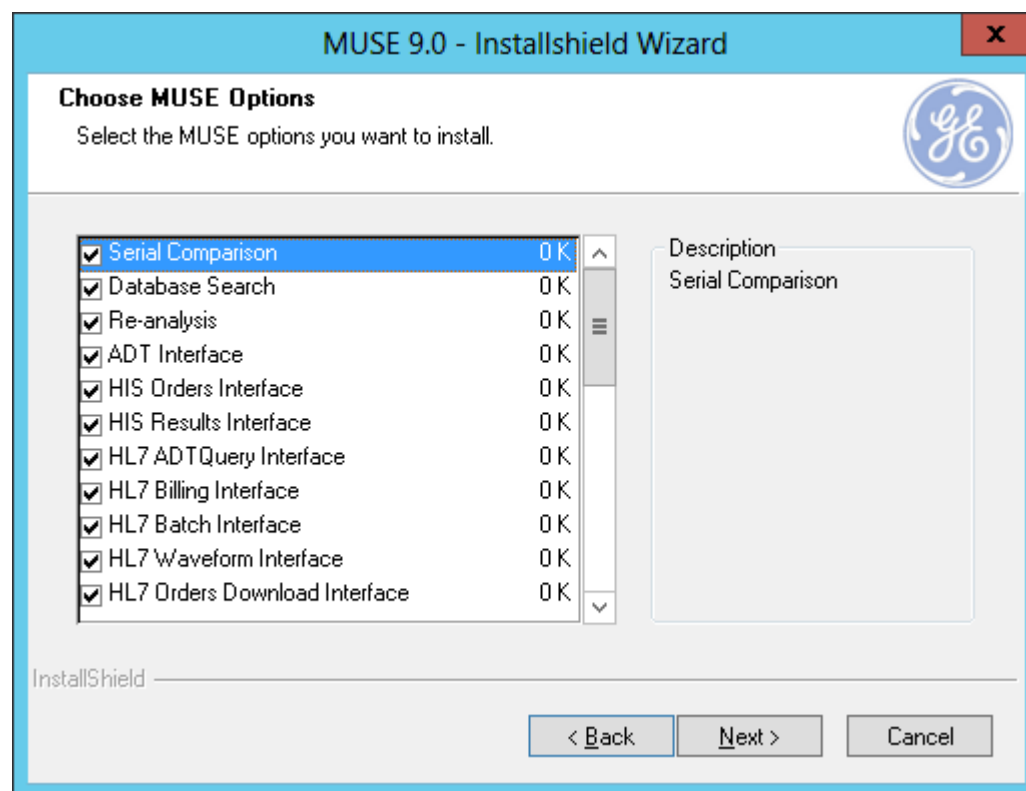
### MUSE CCG DVD

Type	Name	Description
Folder	\MUSE9_CCG	MUSE 9 CCG application files
File	\MUSE9_CCG.iso	ISO of the MUSE 9 CCG application files

## MUSE Options

The MUSE system uses options to enable certain features within the MUSE application.

To view a list of installed options on the system, run the MUSE v9 application in **Modify** mode and view the **Choose MUSE Options** screen. See [“Modifying the MUSE Installed Configuration” on page 59](#) for information regarding running in **Modify** mode.



The following table lists the MUSE options in the order that they are listed in the MUSE InstallShield Wizard. Some options require a corresponding MUSE Service to be installed (see [“MUSE Services” on page 20](#)). An authorized GE Healthcare service representative is the only one who can install the MUSE options. For more information about these options, refer to the *MUSE v9 Cardiology Information System Pre-Installation Manual*.

### MUSE Options

MUSE Option	Description	Related MUSE Service
Serial Comparison	Enables ECG Serial Comparison.	None
Database Search <sup>1</sup>	Enables Database Search.	None
Re-analysis	Enables Re-analysis.	None
ADT Interface	Enables ADT Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Parser
HIS Orders Interface	Enables Order Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Parser

## MUSE Options (cont'd.)

MUSE Option	Description	Related MUSE Service
HIS Results Interface	Enables Results Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Outbound
HL7 ADT Query Interface	Enables ADT Query Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Parser
HL7 Billing Interface	Enables HL7 Billing Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Outbound
HL7 Batch Interface	Enable HL7 Batch Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Outbound
HL7 Waveform Interface	Enables HL7 Waveform Interface. Requires MUSE HL7 Interface (CCG).	MUSE HL7 Outbound
HL7 Orders Download Interface	Enables Order Download Interface. Requires MUSE HL7 Interface (CCG).	None
XML Import	Enables XML Import for MUSE. This is ECG only.	MUSE XML Parser
ACI TIPI <sup>1</sup>	Enables ACI-TIPI features.	None
Wireless/LAN Communication	Enables Wireless/LAN communication features.	MUSE Modem
Email	Enables Email support for MUSE.	MUSE Email
DCP Communication <sup>1</sup>	Enables DCP Communication features.	MUSE DCP Inbound and MUSE DCP Outbound
21 CFR Part 11	Enables 21 CFR Part 11 features.	None
Interval Editor	Enables Interval Editor.	None
XML Export	Enables XML Export for MUSE. This is ECG only.	MUSE File Copy or MUSE FTP Copy
Enhanced Editor	Enables Enhanced Editor.	None
E14 Blinding	Enables E14 Blinding features.	None
HiRes Data Storage <sup>1</sup>	Enable HiRes storage.	None
HiRes P Wave Data Storage	Enable storage of HiRes P Wave data.	None
Exercise Testing Data Storage	Enables storage of Stress Exercise data.	None
Holter Data Storage	Enables storage of Holter data.	None

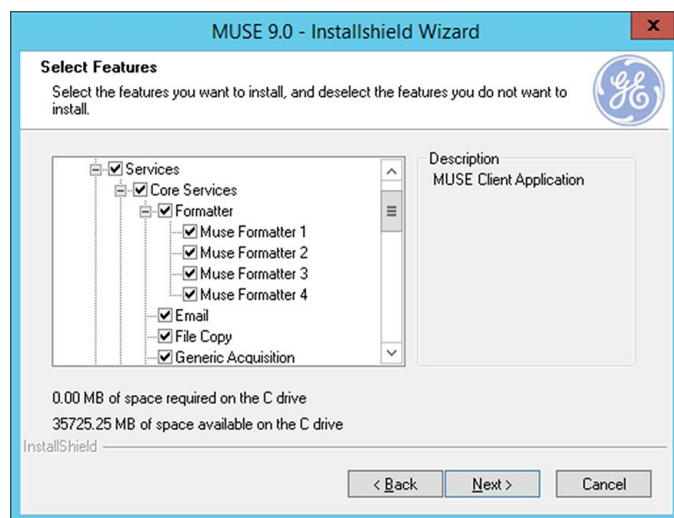
## MUSE Options (cont'd.)

MUSE Option	Description	Related MUSE Service
eDoc Connect	Enables storage of third-party electronic documents.	None
LDAP Authentication	Enables LDAP Authentication features.	None
DICOM	Enables DICOM features.	MUSE DICOM Modality Worklist Client, MUSE DICOM Storage Provider, MUSE Storage User
<sup>1</sup> This option is standard on all MUSE v9 systems.		

## MUSE Services

The MUSE system uses Windows services to perform certain functions within the MUSE application. MUSE services are installed and configured to start using the MUSE Background account.

To view a list of installed services on the system, open Windows services or execute the MUSE v9 **Modify** mode and view the **Select Features** screen. For information to execute MUSE **Modify** mode, see [“Modify the MUSE Installed Configuration” on page 45.](#)



The following table provides a list of MUSE services with a brief description of each. Some services also require a corresponding MUSE option to be installed; related MUSE options are listed in the following table. When troubleshooting specific problems, it may be useful to verify the corresponding service is running.

MUSE v9 includes an Auto Shutdown feature to notify users in advance of a shutdown. For information on how to use this feature, see [“Auto Shutdown” on page 57](#).

### MUSE Services

Service Name	Description	Related MUSE Option(s)
MUSE	MUSE Service Control Manager. When started, all MUSE services are started. When stopped, all MUSE services are stopped. Does not start or stop the MUSEAPI3 service.	None
MUSE DCP Inbound	Listens for inbound DCP communication.	DCP Communication
MUSE DCP Outbound	Used for outbound DCP communication.	DCP Communication
MUSE DICOM Modality Worklist Client	Used to communicate with DICOM Modality Worklist Service Class Provider to retrieve orders.	DICOM
MUSE DICOM Storage Provider	Used to acquire incoming DICOM tests.	DICOM
MUSE DICOM Storage User	Used by outbound DICOM devices in MUSE.	DICOM
MUSE Email	Handles email transmission from MUSE.	Email
MUSE File Copy	Used by outbound folder devices in MUSE. The user account configured to start this service must have appropriate share and file system authorization to create files in the destination specified in MUSE folder device types.	None
MUSE Format 1–4	Formats output to MUSE devices.	None
MUSE FTP Copy	Used by outbound FTP folder devices in MUSE.	None
MUSE Generacq	Acquires data from folders and shares. The user account configured to start this service must have appropriate share and file system authorization to access and delete files specified in the share folders defined within MUSE.	None
MUSE HL7 Outbound	Used by outbound HL7 devices in MUSE.	HL7 Billing Interface, HL7 Batch Interface, HL7 Waveform Interface, HL7 Orders Download Interface
MUSE HL7 Parser 1–4	Listens for inbound HL7 messages.	ADT Interface, HIS Orders Interface, HIS Results Interface, HL7 ADT Query Interface

## MUSE Services (cont'd.)

MUSE Modem	Supports FAX and CSI wireless communication. CSI includes modem, LAN, and wireless CSI.	Wireless and LAN Communication. This option is not required for physical modems.
MUSE MT Host	Handles middle—tier communications between the MUSE clients and the MUSE application server.	None
MUSE Normal	Normalizes tests acquired into MUSE.	None
MUSE Print	Handles printing to Postscript and PCL devices. The user account configured to start this service must have appropriate authorization to access the network printer UNC paths defined in MUSE.	None
MUSE Scheduler	Runs MUSE scheduled tasks.	None
MUSE XML Parser	Handles acquisition of XML data.	XML Import
MUSEAPI3	Used for MUSE API 3 applications. Used by MUSE Web Compatibility Layer and CV Web 3. This service does not start and stop when the MUSE Service Control Manager service is started and stopped.	None

## MUSE v9 Drive Contents and Supporting Folders

The MUSE v9 application and database can be installed on the same server or separate servers. The MUSE application and database supports installation on other drive partitions.

## MUSE Application with Local Database

When installing the MUSE application and database on the same server, the following tables list the recommended installation configurations.

This is the simplest configuration and avoids the need to adjust firewall settings and set permissions between the MUSE server and SQL Server databases.

### C: Drive

Application	Description
Windows OS	Windows Server
Adobe Reader XI	Adobe Reader required to display PDF content. Installed with the MUSE system
SQL Server	Database engine used by the MUSE system
SQL Server Management Studio	Required for support and troubleshooting

## C: Drive (cont'd.)

Application	Description
MUSE	MUSE application folder located in Program Files
InSite ExC	Enables GE Healthcare remote support

## D: Drive (MUSE System)

Folder	Description
db	MUSE databases.
acq	Default path MUSE Generacq service checks for tests. Shared by default for use with CASE/CardioSoft systems.
backup	Supporting files for GE Healthcare tape or network backup. No longer supported as of MUSE v9.
mars	Temporarily stores formatted Holter reports ready for printing.
xml	Temporarily stores inbound XML data (requires <b>XML import</b> option).

## MUSE Application with Remote Database

## MUSE Application Server

Application/Folders	Description
Windows OS	Windows Server.
Adobe Reader XI	Adobe Reader required to display PDF content. Installed with the MUSE system.
SQL Management Studio	Required for access to the 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, \backup, \mars, and \xml.
\acq	Default path MUSE Generacq service checks for tests. Shared by default for use with CASE/CardioSoft systems.
\backup	Supporting files from GE tape or network backup. No longer supported as of MUSE v9.

### MUSE Application Server (cont'd.)

Application/Folders	Description
\mars	Temporarily stores formatted Holter reports ready for printing.
\xml	Temporarily stores inbound XML data (requires <b><i>XML import</i></b> option).

### MUSE Database Server

Application/Folders	Description
SQL Server	Database engine used by the MUSE system.
muse\db	MUSE databases.



# System Setup

Initial setup instructions for the MUSE system are found in the *MUSE v9 Cardiology Information System Operator Manual*.

For information on setting up any of the following items, refer to the *MUSE v9 Cardiology Information Devices and Interfaces Manual*:

- MUSE eDoc Connect
- DICOM Integration
- MAC Carts to MUSE
- CASE to MUSE
- MARS to MUSE
- MUSE Monitoring Gateway
- MUSE XML Import
- MUSE API 3
- MUSE Web Compatibility
- MUSE MACCRA Compatibility
- CardioDay v2.5 to MUSE
- MUSE Configuration for VA VistA Imaging

This chapter provides additional instructions for configuration of the MUSE system after installation is complete. The topics covered in this chapter are:

- [“Configuring Windows High Contrast Color Scheme on MUSE Client”](#)
- [“Changing the Default Rhythm Lead\(s\) in ECG Format Settings”](#)
- [“MUSE Report Distribution Configuration Report \(DumpReportDist.bat\)”](#)
- [“Import and Export Profiles Tool”](#)
- [“Stress List Management”](#)

## Configuring Windows High Contrast Color Scheme on MUSE Client

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

1. From the MUSE client that is being used by a color impaired individual, use **Windows Display > Appearance** settings to activate one of the High Contrast options:
  - High Contrast #1
  - High Contrast #2
  - High Contrast Black
  - High Contrast White
2. From the Windows desktop, copy a MUSE shortcut icon, which was created during installation, and paste it on the Windows desktop.
3. Rename the shortcut by adding **Windows Default Colors** to the end of the name.
4. Right-click on the shortcut and select **Properties**.
5. In the **Target** field, add the following to the end of the string:  
**<space> —nocui**
6. Click **OK** to save your changes.
7. Repeat step 2 through step 6 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 the Default Rhythm Lead(s) in ECG Format Settings

The ECG Format Settings within the MUSE application can be configured to output rhythm leads. For example, the default rhythm leads can be configured in the **ECG Specific Format Properties > Format Styles** screen of the MUSE system.

Format Style	Default Rhythm Lead(s)
4 x 2.5 with 1 Rhythm Lead	V1
4 x 2.5 with 3 Rhythm Leads	V1, II, V5
Pharma 4 x 2.5 with 2 Rhythm Leads	V1, II
Pediatric 5 x 2 with 1 Rhythm Lead	V1
Adult 5 x 2 with 1 Rhythm Lead	V1

A customer can change the default rhythm lead for one or all ECG format settings. Two tools installed with the MUSE system are used to change the default rhythm leads and are installed in the MUSE application folder (default is **c:\Program Files (x86)\MUSE**).

Tool	Description
<b>setlead1.bat</b>	Allows the first default rhythm lead to be changed. For use by format styles that only have 1 rhythm lead.
<b>setlead3.bat</b>	Allows all three default rhythm leads to be changed. For use by format styles that have 2 or 3 rhythm leads.

To execute this command-line tool, perform the following steps:

1. Log on to the MUSE application server as the MUSE administrator user.
2. Launch the Windows **Command Prompt**.
3. Change to the location of the MUSE application folder.
4. Execute either **setlead1.bat** or **setlead3.bat** using the appropriate command-line parameters specified in “[setlead1.bat Tool](#)” on page 27 or “[setlead3.bat Tool](#)” on page 28.

## setlead1.bat Tool

The following tables list the command string to use the tool and provides examples and a description of each example.

Usage:	<b>setlead1 lead1 [-id:&lt;format&gt;] [-server:&lt;server&gt;] [-prefix:&lt;prefix&gt;]</b> where: <b>lead1</b> = I, II, V1, V2, V3, V4, V5, V6, III, AVR, AVL, AVF <b>-id</b> = Format ID (default=all) <b>-server</b> = Name of SQL server and instance <b>-prefix</b> = Prefix for MUSE database
--------	---

Command/Usage Example	Description/Result
<b>setlead1 II</b>	Database server is local. Sets the default rhythm lead for all ECG format settings to II.
<b>setlead1 II -id:6</b>	Database server is local. Sets the default rhythm lead for just the format setting with ID 6 to II.
<b>setlead1 II -id:6 -server:SQLMAIN1</b>	Database server is named <b>SQLMAIN1</b> . Sets the default rhythm lead for just the format setting with ID 6 to II.

## setlead3.bat Tool

The following tables list the command string to use the tool and provides examples and a description of each example.

Usage:	<b><i>setlead3 lead1 lead2 lead3 [-id:&lt;format&gt;] [-server:&lt;server&gt;] [-prefix:&lt;prefix&gt;]</i></b> where: <b><i>lead1</i></b> = I, II, V1, V2, V3, V4, V5, V6, III, AVR, AVL, AVF <b><i>lead2</i></b> = I, II, V1, V2, V3, V4, V5, V6, III, AVR, AVL, AVF <b><i>lead3</i></b> = I, II, V1, V2, V3, V4, V5, V6, III, AVR, AVL, AVF <b><i>-id</i></b> = Format ID (default=all) <b><i>-server</i></b> = Name of SQL server and instance <b><i>-prefix</i></b> = Prefix for MUSE database
--------	--

Command/Usage Example	Description/Result
<b><i>setlead3 V1 V2 V3</i></b>	Database server is local. Sets the default rhythm leads for all ECG format settings to V1, V2, and V3.
<b><i>setlead3 V1 V2 V3 -id:6</i></b>	Database server is local. Sets the default rhythm lead for just the format setting with ID 6 to V1, V2, and V3.
<b><i>setlead3 V1 V2 V3 -id:6 -server:SQLMAIN1</i></b>	Database server is named <b>SQLMAIN1</b> . Sets the default rhythm lead for just the format setting with ID 6 to V1, V2, and V3.

## MUSE Report Distribution Configuration Report (DumpReportDist.bat)

The tool ***DumpReportDist.bat*** is installed with the MUSE system to write the entirety of the MUSE Report Distribution configuration to a file for reference. This tool is installed in the MUSE application folder (default is ***c:\Program Files (x86)\MUSE***).

The tool generates two types of reports: by test type or by device type. The Test Type Report sorts the output of the report distribution configuration by test type. The Device Type Report sorts the output by device number.

To execute this command-line tool, perform the following steps:

1. Log on to the MUSE application server as the MUSE administrator user.
2. Launch the Windows **Command Prompt** using **Run as Administrator**.

3. Change to the location of the MUSE application folder.
4. Execute **DumpReportDist.bat** using the appropriate command-line parameters specified in the following tables.

Usage:	<b><i>DumpReportDist [/r:reportType] [/f:filename] [/db:dbname] [/s:dbserver]</i></b> where: <b><i>/r:reportType</i></b> = 0 for Test Type Report (0 is default), 1 for Device report <b><i>/f:filename</i></b> = Output file name (default is <b><i>ReportDistribution.txt</i></b> in current folder) <b><i>/db:dbname</i></b> = Site database to use in <b><i>MUSE_Sitexxxx</i></b> format (default is <b><i>MUSE_Site0001</i></b> ) <b><i>/s:dbserver</i></b> = Name of the database server (default is <b><i>local</i></b> )
--------	---

Command/Usage Example	Description/Result
<b><i>DumpReportDist /r:0 /f:c:\temp\site1_type.txt /db:MUSE_Site0001</i></b>	Database server is <b><i>local</i></b> . Outputs Test Type report named <b><i>c:\temp\site1_type.txt</i></b> using MUSE Site 1 database.
<b><i>DumpReportDist /r:1 /f:c:\temp\site2_dev.txt /db:MUSE_Site0002 /s:SQLMAIN1</i></b>	Database server is named <b><i>SQLMAIN1</i></b> . Outputs Device report named <b><i>c:\temp\site2_dev.txt</i></b> using MUSE Site 2 database.

## Import and Export Profiles Tool

The MUSE system has a tool to import and export MUSE profiles. This section describes the tool and the processes to import and export profiles.

### Launching the Import and Export Profiles Tool

Launch the tool by running the **ProfileExport.exe** from the MUSE installation folder. Default is **C:\Program Files (x86)\MUSE**.

The tool can be launched from the MUSE application server or a MUSE client workstation.

**NOTE:**

The default authentication mode is Windows. Add **-museauthenticate** to the command-line to run the tool using MUSE Authentication.

## Exporting a Profile

1. Launch the Import & Export Profiles Tool.  
A list of the profiles currently on the MUSE system is displayed.
2. Select the profile to export.
3. Click **Export**.
4. Type the path and file name for the file.
5. Click **Save**.  
The file is saved as an XML file with the name typed in step 4.

## Importing a Profile

1. Create a new profile in the MUSE system.  
This new profile is a place holder for the imported profile information.  
Alternatively, an existing profile may be used instead of creating a new one.  
To create a profile in MUSE, refer to “Profiles” in the *MUSE v9 Cardiology Information System Operator Manual*.
2. Launch the Import & Export Profiles Tool.  
A list of the profiles currently on the MUSE system is displayed.
3. Select the profile that you create in step 1.
4. Click **Import**.
5. Type the path and file name for the file.
6. Click **Open**.  
The Import & Export Profiles Tool copies the imported file and replaces the new profile with the imported file.

## Changing the MUSE CSI Order Download Filtering and Sizing

Change the MUSE CSI Order Download filtering and sizing by using the instructions in the following sections. The changes made here only effect orders downloaded via the CSI protocol. Orders downloaded via other protocols are not effected by these changes.

These instructions manipulate the MUSE database tables and should be performed only by GE Healthcare MUSE Technical Support or a MUSE Field Specialist. The person completing this task should be familiar running queries with SQL Server Management Studio.

## Limiting CSI MUSE Order Downloads by Test Type

By default, when downloading orders from the MUSE system, orders for all test types are included. You can configure the MUSE application to filter the downloading of orders by test type.

Filtering uses the binary bit mask of the number in the **CSITypeDownload** field of the **MUSE\_System.dbo.cfgSites** table. The default value is 0. When the field contains 0, there is no filtering of the orders.

The following table lists the values for each bit mask and defines the filtering scheme.

#### Bit Mask Values for Test Types

Bit	Test Type	Value
1	Resting ECG	1
2	Pacemaker	Not used
3	HiRes	4
4	Stress	8
5	Holter	16

Setting the bit to a value in the bit mask only allows that order type to be sent. To send more than one order type, add the values together and use the sum as the value. For example to send only Resting ECG and HiRes orders, add the values 1 and 4 which equals 5. In this example order types, Stress and Holter, are excluded from the order download. To send only resting ECGs, set the **CSITypeDownload** field to 1.

Use the following procedure, along with the information in the table, to filter which orders can be downloaded from MUSE.

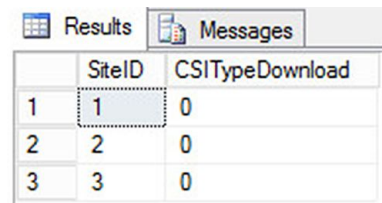
1. Log on to the MUSE application server as the MUSE Administrator user.
2. Execute the following query in **SQL Server Management Studio** to determine the current configuration:

```

--- BEGIN QUERY ---
SELECT SiteID, CSITypeDownload
FROM MUSE_System.dbo.cfgSites
--- END QUERY ---

```

The query returns the current values for each MUSE site.



	SiteID	CSITypeDownload
1	1	0
2	2	0
3	3	0

3. If changes need to be made to the configuration, perform a full or partial shutdown of the MUSE system following the shutdown procedures described in ["Activating System Auto Shutdown" on page 58](#).

4. Execute the following query in **SQL Server Management Studio** to change the filtering value, replacing **X** with the filter value and **Y** with the **SiteID** of the site where the filter is to be applied:

```

--- BEGIN QUERY ---
UPDATE MUSE_System.dbo.cfgSites
SET CSITypeDownload = X
WHERE SiteID = Y
--- END QUERY ---

```

For example, to allow order download for only resting ECG and HiRes on Site 1, add the values **1** and **4**, which equals **5** and run the following query.

```

--- BEGIN QUERY ---
UPDATE MUSE_System.dbo.cfgSites
SET CSITypeDownload = 5
WHERE SiteID = 1
--- END QUERY ---

```

5. Repeat the command for each site that needs to be changed.
6. Verify your changes by re-executing the following query in **SQL Server Management Studio** to determine the current configuration.

```

--- BEGIN QUERY ---
SELECT SiteID, CSITypeDownload
FROM MUSE_System.dbo.cfgSites
--- END QUERY ---

```

7. Cancel the Auto Shutdown following the shutdown procedure [“Canceling the System Shutdown”](#) on page 59.

## Increasing or Decreasing the Number of CSI Order Downloads

By default, when downloading orders from the MUSE system, a total of 100 orders is returned to the requesting device. The MUSE application can be configured to increase or decrease this number of orders.

To change the number of orders that get returned, edit the **CSIMaxOrderDownload** field in the **MUSE\_System.dbo.cfgSites** table. The maximum limit that can be set in the MUSE application is 360. However, cart limitations may prevent this number of orders from being stored. It is strongly recommended that the number of orders be set to not exceed 200.

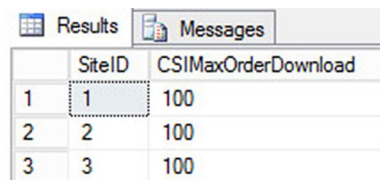


The following procedure can be used to change the number of orders returned by the MUSE system.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Execute the following query in **SQL Server Management Studio** to determine the current configuration.

```
--- BEGIN QUERY ---
SELECT SiteID, CSIMaxOrderDownload
FROM MUSE_System.dbo.cfgSites
--- END QUERY ---
```

The query returns the current values for each MUSE site.



	SiteID	CSIMaxOrderDownload
1	1	100
2	2	100
3	3	100

3. If changes need to be made to the configuration, perform a full or partial shutdown of the MUSE system following the shutdown procedures described in ["Activating System Auto Shutdown" on page 58](#).
4. Execute the following query in **SQL Server Management Studio** to change the maximum value, replacing **X** with the new max value and **Y** with the **SiteID** of the site where the new max is to be applied:

```
--- BEGIN QUERY ---
UPDATE MUSE_System.dbo.cfgSites
SET CSIMaxOrderDownload = X
WHERE SiteID = Y
--- END QUERY ---
```

For example, to allow a maximum value of 150 on Site 1, run the following query

```
--- BEGIN QUERY ---
UPDATE MUSE_System.dbo.cfgSites
SET CSIMaxOrderDownload = 150
WHERE SiteID = 1
--- END QUERY ---
```

5. Repeat the command for each site that needs to be changed.
6. Verify your changes by re-executing the following query in **SQL Server Management Studio** to determine the current configuration.

```
--- BEGIN QUERY ---
SELECT SiteID, CSIMaxOrderDownload
FROM MUSE_System.dbo.cfgSites
--- END QUERY ---
```

7. Cancel the Auto Shutdown following the shutdown procedure [“Canceling the System Shutdown” on page 59.](#)

## Stress List Management

The Stress List Management procedure is intended to provide **limited** management for the selections that appear in the drop-down lists located in the MUSE Editor for stress reports. It is not a standard list management tool. It should be considered an infrequent procedure to adjust the Stress drop-down lists in the MUSE Editor only when necessary.

These instructions manipulate the MUSE database tables and should be performed only by MUSE Technical Support or a MUSE Field Specialist. The person completing this task should be familiar running queries with SQL Server Management Studio.

The strings that appear in the drop-down lists in the MUSE Editor for stress reports are located in the **cfgDataDictUserEnums** table in the **MUSE\_SiteXXXX** database, where **XXXX** represents the MUSE site number.

These strings can be:

String	Definition
Retired	The value no longer displays in the drop-down list.
Unretired	The value displays in the drop-down list.
Sort order changed	The most frequently used values display at the top of the list.

These changes require that values in the **cfgDataDictUserEnums** table be altered.

### NOTE:

Modifying these strings requires customer input. For this reason, the complete list of strings will be copied into an Excel spreadsheet where the changes can be reviewed and approved by the customer prior to applying the changes.

**DO NOT** make any changes to any values other than those described. Existing strings may have been used on past Stress tests and must be maintained as-is. As shown in the following illustration, each drop-down list uses a **FieldID** number that identifies it in the database and each selection in the drop-down has an **EnumString** and **EnumID** number that identifies a specific string in the list.

## New String for Stress Tests

New strings cannot be created using this procedure. New strings are automatically created in the MUSE system based on new strings existing in newly acquired stress tests. The MUSE v9 system automatically sets all new strings to a Retired state. Any new strings sent to the MUSE system do not display in the drop-down lists in the MUSE Editor for use with any stress tests other than the one for which they were originally added. Any new strings that the customer wants to use with the MUSE system must be unretired using this procedure.

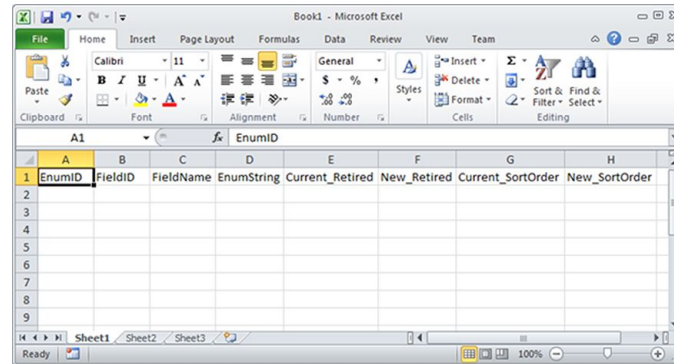
## Creating a Worksheet

1. Create an Excel spreadsheet template with the following columns and save it with an appropriate file name.

For example: **FacilityName\_SiteXXXX\_Stress\_Lists.xlsx**, where XXXX is the appropriate site number.

Column Identifier	Column Heading
A1	EnumID
B1	FieldID
C1	FieldName
D1	EnumString
E1	Current_Retired
F1	New_Retired

Column Identifier	Column Heading
G1	Current_SortOrder
H1	New_SortOrder



2. Log in to the MUSE application server as MUSE administrator.
3. Launch SQL Server Management Studio and log in to the appropriate SQL Server instance.
4. Run the following SQL Query replacing XXXX with the appropriate MUSE site database

```

-- BEGIN QUERY --
SELECT EnumID, FieldID,
FieldName =
CASE FieldID
WHEN '13482' THEN 'Exercise Nurse'
WHEN '13484' THEN 'Attending Physician'
WHEN '13494' THEN 'Test Type'
WHEN '13507' THEN 'Reason For Test'
WHEN '13546' THEN 'Protocol'
WHEN '13590' THEN 'Arrhythmias'
WHEN '13614' THEN 'Resting ECG'
WHEN '13625' THEN 'ST Changes'
WHEN '13655' THEN 'Overall Impression'
WHEN '13663' THEN 'Chest Pain'
WHEN '13952' THEN 'Reason for Termination'
WHEN '13969' THEN 'HR Response to Exercise'
WHEN '13974' THEN 'BP Response to Exercise'
WHEN '13979' THEN 'Functional Capacity'
ELSE 'Unknown'
END,
EnumString, Retired as Current_Retired, '' as New_Retired,
SortOrder as Current_SortOrder, '' as New_SortOrder
FROM MUSE_SiteXXXX.dbo.cfgDataDictUserEnums
WHERE FieldID IN(13482, 13484, 13494 ,13507 ,13546 ,13590
,13614 ,13625 ,13655 ,13663 ,13952 ,13969 ,13974 ,13979)
ORDER BY FieldID
-- END QUERY --

```

- Paste the results of the query into the template Excel file you created in Step 1 starting with cell A2.

EnumID	FieldID	FieldName	EnumString	Current_Retired	New_Retired	Current_SortOrder	New_SortOrder
781	13507	Reason For 'Abnormal E		0		1	
782	13507	Reason For 'Abnormal E		0		2	
783	13507	Reason For 'Suspected A		0		3	
784	13507	Reason For 'Screening fc		0		4	
785	13507	Reason For 'Dyspnea		0		5	
786	13507	Reason For 'Dyspnea wit		0		6	
787	13507	Reason For 'Evaluation o		0		7	
788	13507	Reason For 'Fatigue		0		8	

6. Save the Excel file and send it to the customer with the following instructions:
  - a. Populate column F (New\_Retired) with a value of 0 for unretired or a value of 1 for retired.
  - b. Populate column H (New\_SortOrder) with the desired sort order value.  
Sort Order values should not be duplicated within a range of FieldNames. Anything marked as retired in column F must have a New\_SortOrder value of 500.
7. After you obtain the completed Excel file from the customer, verify that every row has a value of 0 or 1 for column F (New\_Retired) and a numeric value in column H (New\_SortOrder).
8. Using the values in these columns, follow the instructions in the ["Retiring Strings"](#), ["Unretiring Strings" on page 38](#), and ["Changing the Sort Order of Strings" on page 38](#) to implement the changes.

## Retiring Strings

To retire a string, run the following query, replacing XXXX with the appropriate MUSE site database and YYYY with the appropriate EnumID:

```
-- BEGIN QUERY --
UPDATE MUSE_SiteXXXX.dbo.cfgDataDictUserEnums
SET Retired = 1, SortOrder = 500
WHERE EnumID = YYYY
-- END QUERY --
```

## Unretiring Strings

To unretire a string, run the following query, replacing XXXX with the appropriate MUSE site database and YYYY with the appropriate EnumID:

```
-- BEGIN QUERY --
UPDATE MUSE_SiteXXXX.dbo.cfgDataDictUserEnums
SET Retired = 0
WHERE EnumID = YYYY
-- END QUERY --
```

## Changing the Sort Order of Strings

To change the sort order of a string, run the following query, replacing XXXX with the appropriate MUSE site database, YYYY with the appropriate EnumID, and ZZZZ with the appropriate SortOrder value:

```
-- BEGIN QUERY --
UPDATE MUSE_SiteXXXX.dbo.cfgDataDictUserEnums
SET SortOrder = ZZZZ
WHERE EnumID = YYYY
-- END QUERY --
```

## Combining Unretire and Changing Sort Order Queries

A single query can be used to both unretire and change the sort order. To unretire and change the sort order of a string at the same time, run the following query, replacing XXXX with the appropriate MUSE site database, YYYY with the appropriate EnumID, and ZZZZ with the appropriate SortOrder value:

```
-- BEGIN QUERY --
UPDATE MUSE_SiteXXXX.dbo.cfgDataDictUserEnums
SET Retired = 0, SortOrder = ZZZZ
WHERE EnumID = YYYY
-- END QUERY --
```

## Correcting Mistakes

Since these queries only impact the Retired and/or SortOrder columns of the **cfgDataDictUserEnums** table, if any mistakes are made during the process, those mistakes can be corrected by running the appropriate queries to change the sort order, retire, or un-retire the string as appropriate. The original Excel file created in [“Creating a Worksheet” on page 35](#) can be used as a reference for the original configuration of the strings.





## MUSE Service Users

This chapter describes the following items:

- MUSE service user requirements, including Windows user account requirements and SQL Server Login and user requirements
- How to change the MUSE user passwords
- How to change the Windows user accounts and passwords used with the MUSE system
- How to configure SQL Server security

## MUSE Service User Accounts

The MUSE service accounts, comprised of MUSE user accounts and Windows user accounts, are integral to the correct operation of the MUSE system. The following table identifies the accounts:

Account	Default Account Name	Description
MUSE Administrator	MuseAdmin	<p>The MUSE Administrator account is used by GE Healthcare service personnel to</p> <ul style="list-style-type: none"> <li>• Log on to the MUSE system to perform initial setup and configuration</li> <li>• Provide ongoing service and support.</li> </ul>
MUSE Background	MuseBkgnd	<p>The MUSE Background account is used to</p> <ul style="list-style-type: none"> <li>• Start the MUSE related background services on the MUSE application server and MUSE client with the MUSE Modem feature</li> <li>• Create new MUSE site databases.</li> </ul>

## MUSE User Accounts

The default MUSE Administrator and MUSE Background accounts are automatically set up as users within the MUSE application. These accounts are critical to the internal working of the MUSE system and cannot be changed, with the exceptions of their passwords and Windows user names. The MUSE user service accounts are linked to the Windows user service accounts through the **Windows User Name** field in MUSE

user setup. This linkage happens automatically by the MUSE installer and should only be changed by re-installing the MUSE system or using the MUSE Modify mode.

The MUSEAdmin and MUSEBkgnd user accounts in the MUSE system have known default passwords. The customer should change these passwords for these users. To change the MUSE system passwords for these accounts, see [“Changing the MUSE Service Account Passwords in the MUSE System” on page 44.](#)

## Windows User Accounts

The Windows MUSE Administrator and MUSE Background accounts provide access to the MUSE application, MUSE services, and SQL Server databases. They are linked to the MUSE user accounts.

These user names and passwords must meet the following requirements:

- Must be a member of the local **Administrators** group on the MUSE application server.  
The MUSE Background user must also be a member of the local **Administrators** group on any MUSE client workstations where the MUSE Modem feature will be used.
- Must have appropriate access to the MUSE databases on the SQL Server instance where the MUSE databases are located. See the table in [“SQL Server Role Requirements” on page 43.](#)
- Should be a domain account whenever possible to avoid mismatches of local account user name and passwords.
- Set passwords to never expire, whenever possible. If the passwords change, GE Healthcare service personnel might not be able to log on to the system to provide support. Additionally, the background services can fail to start, causing the MUSE system to stop functioning.
- Allow the customer to determine both the account names and passwords. The passwords must be shared with GE Healthcare service personnel to use the account when they work on the MUSE system.
- The customer should not use the MUSE Administrator or MUSE Background accounts for accessing the MUSE application server or MUSE system. Instead, separate MUSE and/or Windows user accounts should be created for each individual user accessing the MUSE system.

Additionally, the MUSE Background account must not be subject to any policies that would not grant the permissions to the account for **Log on as a service**. **Log on as a service** permission is a requirement for the account to be able to start the MUSE-related background services.

### NOTE:

The MUSE installer grants the MUSE Background account the **Log on as a service** permission on new installations, however, if **MUSE Modify** mode is used to change the MUSE Background user on a client workstation, you need to manually grant the MUSE Background account the **Log on as a service** permission.

### NOTE:

If LDAP/AD authentication is going to be used with MUSE, the Windows User Name for the MUSE Background user must contain the string `MuseBkgnd` somewhere in it. For example: `MuseBkgnd`, `XYZMuseBkgnd`, `MuseBkgndXYZ`, or `XYZMuseBkgndXYZ`.

## SQL Server Role Requirements

The following table provides SQL Server role requirements for the MUSE Administrator and MUSE Background user. For detailed information on implementing these SQL Server roles, see [“Configuring SQL Server Security” on page 47](#).

### SQL Server Role Requirements

Account	SQL Server Role Requirements
MUSE Administrator	SQL Server Login with the <b>sysadmin server role</b> on the SQL Server instance where the MUSE databases are located. This is the preferred configuration for a local database. <i>or</i> SQL Server Login with the <b>public server role</b> on the SQL Server instance where the MUSE databases are located, and database user with <b>db_owner database role</b> for all of the MUSE databases. This configuration is more common for a remote database.
MUSE Background	SQL Server Login with the <b>sysadmin server role</b> on the SQL Server instance where the MUSE databases are located. This is the preferred configuration for a local database. <i>or</i> SQL Server Login with the <b>dbcreator server role</b> on the SQL Server instance where the MUSE databases are created, and database user with <b>db_owner database role</b> for all of the MUSE databases. This configuration is more common for a remote database.

#### NOTE:

It is not possible to give **db\_owner database role** access to the MUSE Administrator or MUSE Background account until the MUSE databases are created

When the MUSE database is installed or upgraded, the MUSE installer automatically attempts to set the MUSE databases owner to the MUSE Background account specified and give **db\_owner** database role to the MUSE Administrator account specified.

## MUSE InstallShield Wizard Requirements

The following table provides Windows and SQL Server requirements for the user who executes the MUSE InstallShield Wizard:

InstallShield Mode	Requirements
Initial Install or Upgrade Mode	<ul style="list-style-type: none"> <li>• Must be a local administrator of the MUSE application server.</li> <li>• Must have SQL Server Login with the <b>sysadmin server role</b> on the SQL Server instance where the MUSE databases are created and reside.</li> <li>• Must have <b>Master</b> configured as the default database for the SQL Server login.</li> </ul>
MUSE Modify Mode	<p>SQL Server Login with the <b>sysadmin server role</b> on the SQL Server instance where the MUSE databases reside. This is the preferred configuration for a local database.</p> <p>OR</p> <p>SQL Server Login with the <b>public server role</b> on the SQL Server instance where the MUSE databases are located, and database user with <b>db_owner database role</b> for all of the MUSE databases. This configuration is more common for a remote database.</p> <p><b>NOTE:</b> If the MUSE Administrator and MUSE Background requirements have been met, either user can be used to execute MUSE Modify mode.</p>

## Changing MUSE Service Accounts

This section describes how to change the MUSE user account passwords and how to change the Windows user accounts and passwords used with the system.

### Changing the MUSE Service Account Passwords in the MUSE System

To change the password of the **MUSE Administrator** or **MUSE Background** 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 you want to change and select **Properties**.  
The **User Properties** window opens.
4. Type a new password in the **MUSE Password** and **Re-enter MUSE Password** fields.
5. Click **OK** to save your change.

## Changing the MUSE Service Accounts and Passwords in Windows

The process to change the Windows user accounts and passwords consist of the following high-level steps:

1. Change or create the Windows accounts and passwords using Windows.
2. Verify SQL Server Logins and Roles.
3. Shut down the MUSE services.
4. Modify the MUSE installed configuration to:
  - Update the MUSE services with the new user name and password.
  - Update the Windows user name of the **MUSE Administrator** and **MUSE Background** user accounts.
5. Cancel the Auto Shutdown.
6. Update the **MUSEAPI3** service user and password, if necessary.

### Change or Create Windows Accounts

The hospital MUSE system and IT administrators are responsible for creating the Windows accounts and passwords. The Windows account user names and passwords used by the new MUSE Administrator and MUSE Background users must be set up and be ready to use before entering them into MUSE. Confirm that the user accounts to be used for the MUSE system meet the requirements specified in [“Windows User Accounts” on page 42](#).

### Verify SQL Server Logins and Roles for MUSE Administrator and MUSE Background Users

**NOTE:**

If only the Windows user passwords are changing, disregard this section .

The hospital MUSE and IT administrators are responsible for ensuring the MUSE Service Users have appropriate SQL Server Logins and Roles. Confirm that the user accounts used for the MUSE system meet the requirements specified in [“SQL Server Role Requirements” on page 43](#).

### Shut Down the MUSE Services

Perform the following steps to shut down the MUSE services.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full shutdown of the MUSE system using the instructions in [“Activating System Auto Shutdown” on page 58](#).

Notify all user that the system is being shut down for maintenance.

### Modify the MUSE Installed Configuration

After changing or creating the Windows Accounts and Verifying SQL Logins, the MUSE installed configuration needs to be modified with the new accounts and/or passwords.

Perform the following steps on the MUSE application server and any MUSE client or modem servers that have the MUSE Modem feature installed:

1. Log on to Windows:

Point of Access	Log on as
MUSE Application Server	MUSE Administrator user
MUSE Client Workstation	Local administrator

2. Confirm the MUSE application is closed.
3. Go to **Control Panel > Programs and Features**.
4. Select **MUSE 9** and click **Change**.  
The **Welcome...** window opens.
5. Select **Modify** and click **Next**.  
The **Select Feature** windows opens.
6. Click **Next**.
7. If the following prompt is displayed, **SQL server 2008 or SQL server 2008 R2 or SQL server 2012 or SQL server 2014 is not installed. This warning can be ignored if you are installing the MUSE database on a different machine. Do you want to continue?**, click **Yes**.  
The **MUSE Client Configuration** window opens.
8. Click **Next** through each window until the **MUSE Services Configuration** window opens.
9. Type the user name and password for the **MUSE Background** account and the user name for the **MUSE Administrator** account.
  - If you are using a domain account, type the user name in **<domain name>\<user name>** format.
  - If you are using a local account, type the user name in **.\<user name>** format.

No password is required for the MUSE Administrator user account.

**NOTE:**

The MUSE Administrator **User Name** Field is not present when modifying the MUSE configuration on a MUSE client.

Using the **MUSE Background** account and password that you entered in this step, the MUSE installer completes the installation of the MUSE Services . When you perform these steps on the MUSE application server, the MUSE installer also populates the **MUSE Background** and **MUSE Administrator** accounts in the MUSE database with these same Windows user names and passwords.

10. Click **Next**.  
The installer validates that the user accounts that you configured do exist on the system. If you receive a warning message that the account was not found or user validation failed, click **No** at the prompt to return to the **Services Configuration** window and check the following:
  - The user name for the accounts and the password are correct.
  - The accounts exist.

11. Click **Next** until the **Maintenance Complete** window opens.
12. Click **Finish**.

## Cancel the Auto Shutdown

Perform the following steps to cancel the Auto Shutdown and ensure that MUSE services are started.

1. Cancel the MUSE shutdown using the instructions in [“Canceling the System Shutdown” on page 59](#).
2. Verify all MUSE services have started.

## Update the MUSEAPI3 Service

Only use these steps if the **MUSEAPI3** service is installed.

1. Log on to the MUSE application server as an administrator.
2. Go to **Windows Services > MUSEAPI3 > Properties**.
3. Select the **Log On** tab.
4. Change the following fields to match the user account and password for the **MUSE Background** user.

- **This account**
- **Password**
- **Confirm password**

Use the same user account and password that was used to modify the MUSE installed configuration in [“Modify the MUSE Installed Configuration” on page 45](#).

5. Click **OK**.
6. Restart the **MUSEAPI3** service.

## Configuring SQL Server Security

As indicated in the [“SQL Server Role Requirements” on page 43](#), specific SQL Server security requirements must be met for the MUSE Administrator and the MUSE Background users. This section describes the process for configuring SQL Server security.

This section provides specific procedures for completing certain tasks in SQL Server Management Studio. There are multiple ways to perform these same tasks. A customer SQL administrator can perform these tasks in a way that is different from the procedures described here.

## MUSE Background User Access Information

When the MUSE databases are installed or upgraded, the MUSE Background user is made the owner of the MUSE databases. This ensures that the MUSE Background user has a SQL database user created for all the MUSE databases and that the user has the **db\_owner** database role for all of the MUSE databases. If the databases are moved or

reattached, the owner can change. In which case, the **MUSE Background** account may no longer have **db\_owner** access to the database.

## Create a SQL Server Login

The core requirement for all users that need access to a SQL Server instance is a SQL Server login. The following steps can be used to create a SQL Server login. For remote SQL Server instances, the customer's SQL administrator may need to perform these steps:

1. Using **SQL Server Management Studio**, log on to the appropriate SQL Server instance using a SQL Server login with **sysadmin server role** access.
2. In **Object Explorer**, expand the database server.
3. Right-click **Security** and go to **New > Login....**
4. Make sure the **General** page is selected.
5. Select **Windows Authentication**.
6. In the **Login name** field, type the Windows username in **<domain>\<username>** format of the Windows user to create the SQL Server login.  
You can also use **Search...** to locate the user you want to add.
7. Click **OK**.

## Assign SQL Server Roles to a Login

Use the following steps to assign SQL Server Roles to a SQL login. For remote SQL Server instance, the customer's SQL administrator might need to perform these steps.

1. Using **SQL Server Management Studio**, log on to the appropriate SQL Server instance using a SQL Server login with **sysadmin server role** access.
2. In **Object Explorer**, expand the database server.
3. Navigate to and expand **Security > Logins**.
4. Right-click on the login you want to assign the SQL Server roles to and choose **Properties**.
5. Select the **Server Roles** page.
6. Select any Server roles you want to assign to the SQL Server login.  
**NOTE:**  
The **public server** role is always selected and cannot be cleared.
7. Click **OK**.



## Create SQL Server Database Users and Assign Roles

Use the following steps to create SQL Server database users and give them **db\_owner** database role access to the MUSE databases. For remote SQL Server instance, the customer's SQL administrator might need to perform these steps.

**NOTE:**

These steps cannot be performed if the MUSE databases do not currently exist in SQL Server.

1. Using **SQL Server Management Studio**, log on to the appropriate SQL Server instance using a SQL Server login with **sysadmin server role** access.
2. In **Object Explorer**, expand the database server.
3. Navigate to and expand **Security > Logins**.
4. Right-click on the login you want to assign the SQL Server roles to and choose **Properties**.
5. Select the **User Mapping** page.
6. In the **Users mapped to this login** section of the window, select **MUSE\_System**.
7. In the **Database role membership for: MUSE\_System** section of the window, select **db\_owner**.
8. Repeat step 6 through 7 for each of the remaining MUSE databases (**MUSE\_SiteTemplate**, **MUSE\_Site0002**, **MUSE\_Site0003**, and so on.)
9. Click **OK**.



# Application Authentication

The MUSE system supports four methods for application authentication:

- MUSE authentication
- Windows authentication
- LDAP authentication
- Windows and LDAP authentication

The following sections cover the different methods of authentication and how they are configured. For more information on authentication methods, refer to the *MUSE v9 Cardiology Information System Advance Security Guide*.

## MUSE Authentication

This section describes MUSE authentication as well as how to enable and disable it.

### Description

In MUSE authentication, when the user launches the MUSE application after logging onto Windows, the logon screen displays in the MUSE application, and the user needs to provide their MUSE system user name, password, and the site in the system that they want to log onto, if it is other than their default site.

This method can be ideal on shared computers, where the users do not want to log out of the operating system to allow someone else to log into the MUSE application.

MUSE authentication is enabled by default in the MUSE system. MUSE authentication requires a valid MUSE user account.

## Enabling and Disabling MUSE Authentication

MUSE authentication can be enabled or disabled by performing the following procedure:

### NOTE:

If MUSE authentication is disabled, users can only access MUSE using Windows and/or LDAP authentication. For information on creating MUSE user accounts, refer to the *MUSE v9 Cardiology Information System Operator Manual*.

1. Log on to the MUSE application.
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. Perform one of the following:
  - To enable MUSE authentication, select **Allow users to logon using MUSE authentication**.
  - To disable MUSE authentication, clear **Allow users to logon using MUSE authentication**.
6. Click **OK** to save your changes.

## Windows Authentication

This section describes Windows authentication. It provides instructions on how to enable and disable Windows authentication and to map a MUSE user account to a Windows user account.

### Description

In Windows authentication, when the user launches the MUSE application after logging onto Windows, the MUSE application recognizes the user's Windows logon and automatically logs the user into the MUSE application as the appropriate MUSE system user.

This setup requires the Windows domain and user credentials be entered into the user's setup in the MUSE application. No Windows password information is required for this setup. This method is common on computers that are not shared by others, and where the user does not want to have to log on to the MUSE application separately.

### Enabling and Disabling Windows Authentication

Windows authentication is enabled by default in the MUSE system and cannot be disabled. Windows authentication requires a valid Windows user account be mapped to a MUSE user account. If this mapping does not exist, Windows authentication will not work.

### Mapping MUSE User Account to a Windows User Account for Windows Authentication

For information on creating MUSE user accounts, refer in the *MUSE v9 Cardiology Information System Operator Manual*.

Perform the following procedure to map a MUSE user account to a Windows user account:

1. Log on to the MUSE application.
2. Go to **System > Setup**.
3. From the navigation panel, select **Users**.

4. Right-click on the MUSE User to be mapped and choose **Properties**.  
The **User Properties** window opens.
5. In the **Windows User Name** field, type the Windows user name to map to this MUSE user in the format **<domain name>\<user name>**.
6. Click **OK** to save your changes

**NOTE:**

It is not recommended to use MUSE User Setup to change the Windows username for the **MuseAdmin** or **MuseBkgnd** user accounts in the MUSE application. To change the Windows username of these accounts, use **MUSE Modify** mode.

## LDAP Authentication

This section describes LDAP authentication as well as how to enable and disable it.

### Description

Lightweight Directory Access Protocol (LDAP) authentication allows for a more centralized administration of MUSE system users and roles by configuring the MUSE system to be able to communicate with the LDAP server. Microsoft's Active Directory Server makes use of LDAP versions 2 and 3.

With this method, when the user launches the MUSE application after logging onto Windows, the MUSE application logon screen opens, where the user needs to provide their LDAP/Active Directory (AD) username and password, and the site in the system that they want to log onto, if it is other than their default site.

This method can be ideal on shared computers, where the users do not want to log out of the operating system to allow someone else to log onto the MUSE application with LDAP/AD credentials.

This setup requires LDAP be appropriately configured with the MUSE application. Before enabling the LDAP feature, talk with your field representative or technical support specialist.

See [Appendix C](#) for detailed information on configuring the MUSE system for LDAP authentication.

LDAP authentication is disabled by default in the MUSE system. LDAP authentication requires proper configuration to work properly.

## Enabling and Disabling LDAP Authentication

LDAP authentication can be enabled or disabled by performing the following:

1. Log on to the MUSE application.
2. Go to **System > Setup**.
3. From the navigation panel, select **System**.
4. Right-click on the MUSE user to be mapped and select **Properties**.  
The **System Properties** window opens.
5. Select **LDAP Configuration**.

6. Perform one of the following:
  - To enable LDAP authentication, select **Allow users to login using LDAP authentication**.
  - To disable LDAP authentication, clear **Allow users to login using LDAP authentication**.
7. Click **OK** to save your changes.

**NOTE:**

Make sure you do not lock yourself out of the system. You can get locked out as follows:

- If users are currently using Windows authentication and you enable LDAP before it is fully configured. Make sure you configure LDAP according to the procedure in [Appendix C](#).
- If users are currently using MUSE authentication and you turn off MUSE authentication and enable LDAP before it is fully configured. Make sure you configure LDAP according to the procedure in [Appendix C](#).

## Windows + LDAP Authentication

Windows + LDAP authentication is a combination of the LDAP and Windows authentication methods. When configuring Windows + LDAP authentication, all the information for both Windows authentication and LDAP authentication applies to Windows + LDAP authentication.

To access the MUSE system using Windows + LDAP authentication, LDAP must be enabled and the Windows authentication shortcut must be used.

## MUSE Shortcuts

The command-line parameter used when starting the MUSE application components dictates the authentication method used with the MUSE system. Shortcuts are automatically created by the MUSE installer, however, they can also be created and modified manually.

## Using MUSE InstallShield Wizard to Create MUSE Shortcuts

The following procedure explains how to create MUSE shortcuts using the InstallShield wizard in MUSE Modify mode. You can also create shortcuts during installation/upgrade of the MUSE at the **MUSE Client Configuration window**.

1. Log on to the MUSE application server as an administrator.
2. Go to **Control Panel > Programs and Features**.
3. Select **MUSE 9** and click **Change**.  
The **Welcome...** window opens.
4. Select **Modify** and click **Next**.  
The **Select Feature** window opens.
5. Click **Next**.  
The **MUSE Client Configuration** window opens.

6. Select the desired shortcut options on the **MUSE Client Configuration** window using the information in the following table:

Item	Description	Desktop Shortcut Name
<b>Add Windows authentication shortcuts</b>	Select if you want to add Windows authentication shortcuts for MUSE.  <b>NOTE:</b> Select this option when using Windows + LDAP authentication.	MUSE Editor
<b>Add MUSE authentication shortcuts</b>	Select if you want to add MUSE authentication shortcuts for MUSE.	MUSE Editor (MUSE Logon)
<b>Add LDAP authentication shortcuts</b>	Select if you want to add LDAP authentication shortcuts for MUSE.	MUSE Editor (LDAP Logon)

**NOTE:**

You can have either **Add Windows authentication shortcuts** or **Add LDAP authentication shortcuts** selected, but not both.

7. Click **Next** until all your changes are applied and the **Maintenance Complete** window opens.
8. Click **Finish**.

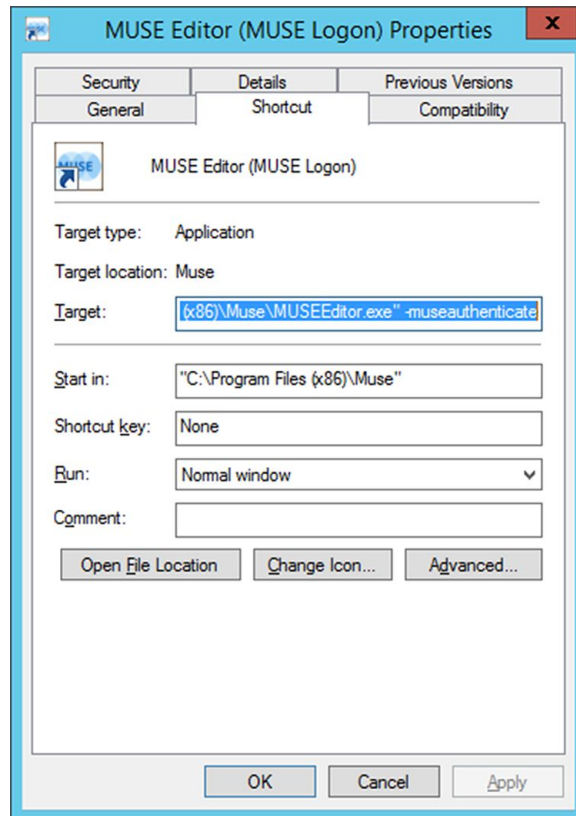
## Manually Modifying MUSE Shortcuts

The command-line parameter of the Windows shortcut tells the MUSE system which authentication method to use. Rather than use the **MUSE Modify** mode to modify MUSE shortcuts, shortcuts can be modified manually by using the following steps.

1. Right-click on an existing MUSE shortcut and choose **Properties** or create a new shortcut in Windows.
2. Select the **Shortcut** tab.
3. In the **Target** field, use the information in the following table to add or remove the command-line parameter as appropriate:

Authentication Method	Command-Line Parameter
<b>Windows authentication or Windows + LDAP authentication</b>	None.  No command-line parameter indicates the authentication method is Windows authentication. This also is the configuration when using Windows + LDAP authentication.
<b>MUSE authentication</b>	<b>-museauthenticate</b>
<b>LDAP authentication</b>	<b>-ldapauthenticate</b>

The following screen shows the parameters for a shortcut configured for MUSE authentication.





# System Administration

This chapter provides procedures for administrative functions in the MUSE system.

## Auto Shutdown

The MUSE Auto Shutdown feature notifies users currently logged on to the MUSE system up to five minutes in advance that the MUSE system is shutting down.

To activate this feature, MUSE system users must have the **Shutdown** privilege enabled for their role. Roles that have this privilege by default include:

- MUSE Service
- System Owner
- Site Manager

For information on completely shutting down the MUSE system, see [“Safe Shutdown Procedures” on page 73](#).

There are two types of shutdown:

- **Full Shutdown**
  - Shuts down all MUSE services on the MUSE application server and MUSE clients.
  - The MUSE application cannot launch from the MUSE client or the MUSE application server.
  - MUSE API 3 applications do not function, including MUSE Web Compatibility Layer and CV Web 3.
- **Partial Shutdown**
  - Shuts down MUSE client applications running remotely.
  - The MUSE services on the MUSE application server continue to run.
  - MUSE application only can be launched from the MUSE application server.
  - MUSE API 3 applications do not function, including MUSE Web Compatibility Layer and CV Web 3.

**NOTE:**

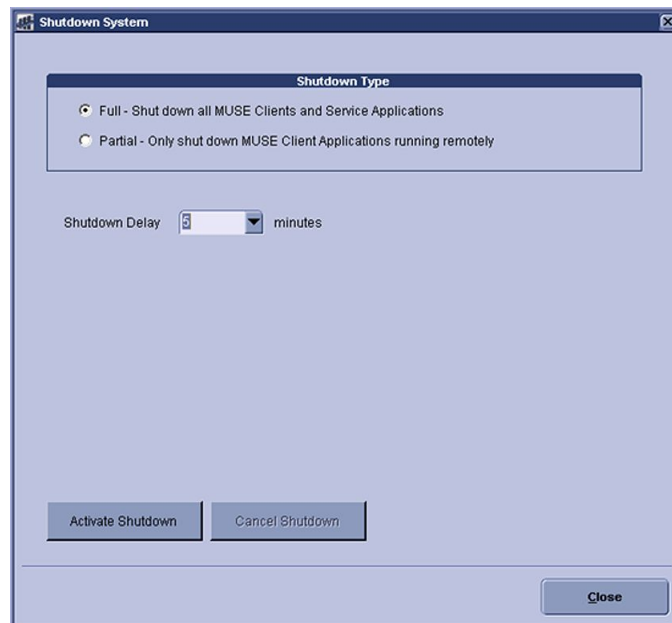
Initiating a Full or Partial Shutdown requires that the shutdown be canceled. If the MUSE service is restarted or the MUSE system is rebooted, only the MUSE and MUSE MT Host service starts until the shutdown is canceled. For information on how to cancel the shutdown, see [“Canceling the System Shutdown” on page 59](#).

## Activating System Auto 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 is shutting down.

6. Close the message window.

The top of the MUSE client application displays a countdown in minutes before the shutdown occurs.



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

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 a remote client, it stops responding and the window automatically closes. Auto Shutdown 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 MUSE application server.

**NOTE:**

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

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



2. In the MUSE application, go to **System > Setup**.
3. On the navigation pane, select **System**.
4. Right-click on the **Product name** and click **Shutdown System**.

The **Shutdown System** window opens.

5. 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 v9 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.
- Changing the Windows accounts and passwords.
- Changing the MUSE port number.

Use the following procedure to change an existing configuration.

1. Log on to the system as MUSE administrator.
2. 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 shut down for maintenance.
3. Close the MUSE client application on the server.
4. Go to the **Control Panel > Programs and Features**.
5. Select the **MUSE 9** entry and click **Change**.  
The MUSE InstallShield launches.
6. Verify that **Modify** is selected, and click **Next**.

7. 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.

8. If no changes are required for a setup window, click **Next** to advance to the next window.

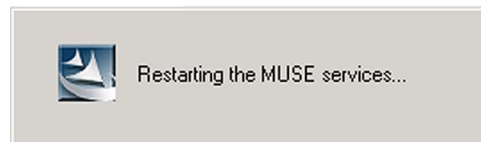
The last window to open is **MUSE Serial Number**.

**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 Auto Shutdown using the instructions in ["Canceling the System Shutdown" on page 59](#).

## Moving the MUSE Databases

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

1. Preparing the new database server
2. Shutting down MUSE services
3. Moving the MUSE databases to the new database server
4. Updating the MUSE database server configuration
5. Canceling the Auto Shutdown
6. Re-installing the MUSE API 3.1

### Preparing the New Database Server

Perform the following steps to prepare the new database server.

1. Create the new SQL Server instance where the MUSE databases are to be moved.
2. Create a folder on the SQL Server where the databases are to be copied.

**NOTE:**

The SQL Server version where the databases are moved must be compatible with MUSE v9 and be the same or higher version of SQL Server currently being used. For example, if the SQL Server currently being used is SQL Server 2008, the database can be moved to SQL Server 2008 or higher. However, if the SQL Server currently being used is SQL Server 2012, the MUSE database cannot be moved to SQL Server 2008 or 2008 R2.

## Shutting Down MUSE Services

Perform the following steps to shut down the MUSE services.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full shutdown of the MUSE system using the instructions in [“Auto Shutdown” on page 57](#).

Notify all users that the system is being shut down for maintenance.

3. After the Auto Shutdown is complete, stop all MUSE services on the MUSE application server.
4. Set the MUSE service **Startup Type** to **Manual**.

This step prevents any MUSE services starting if the system is rebooted.

## Moving the MUSE Databases to the New Server

Moving the MUSE databases to the new server consists of the following steps:

1. Detach the MUSE databases from the old server.
  - a. Log on to the MUSE application server as a user with sysadmin server role access to the current database server.
  - b. Open **SQL Server Management Studio** and connect to the current MUSE database server.
  - c. Expand the database object.
  - d. Right-click on the **MUSE\_System** database, select **Tasks**, and click **Detach**.
  - e. On the **Detach Database** window, confirm the name of the database you are detaching, put a check in the **Drop Connections** check box, and click **OK**.
  - f. Repeat step [d](#) and step [e](#) for each MUSE database.  
(**MUSE\_Site Template**, **MUSE\_Site0001**, **MUSE\_Site0002**, etc.)
2. Copy the MUSE databases to the new server.
  - a. Copy all of the MUSE database files from the old database server to new database server.
  - b. Verify all of the database files were successfully copied. The following table lists the database files that need to be copied for each database.

Database	Database Files
MUSE_System	MUSE_System.LDF MUSE_System.MDF MUSE_System_Config.NDF MUSE_System_MuseLog.NDF MUSE_System_Queue.NDF MUSE_System_QueueBlob.NDF
MUSE_SiteTemplate	MUSE_SiteTemplate.LDF MUSE_SiteTemplate.MDF MUSE_SiteTemplate_Config.NDF MUSE_SiteTemplate_Test.NDF MUSE_SiteTemplate_TestBlob.NDF
Muse_Site0001	MUSE_Site0001.LDF MUSE_Site0001.MDF MUSE_Site0001_Config.NDF MUSE_Site0001_Test.NDF MUSE_Site0001_TestBlob.NDF

**NOTE:**

If any site databases other than **MUSE\_Site0001** exist, those files also need to be copied. The files for additional sites are in the same file name conventions as **MUSE\_Site0001**.

3. Attach the MUSE databases to the new server.

Attaching the database to a remote database server is the responsibility of the customer and the following procedure can be used as a guide. The specific steps for attaching the database to a remote database server can vary depending on the customer's SQL Server implementation.

- a. Open **SQL Server Management Studio** and connect to the new MUSE database server.
- b. Right-click on the **Database** object and select **Attach**.
- c. On the **Attach Database** window, click **Add**.
- d. Browse to the location of the MUSE databases.
- e. Select the **MUSE\_System.mdf** file.
- f. Click **OK** to attach the file.

The selected database is listed in the **Databases to attach** window.

- g. Repeat step **d** through step **f** for each MUSE database. (**MUSE\_SiteTemplate.MDF**, **MUSE\_Site0001.MDF**, **MUSE\_Site0002.MDF**, etc.).

- h. After all of the MUSE databases are listed in the **Databases to attach** window, click **OK**.

**NOTE:**

If an error occurs attaching the database(s) and you are certain all the database files are present and accounted for, you may need to run SQL Server Management Studio using the **Run as administrator** function to attach the databases.

A symptom of needing to use the **Run as administrator** function is the error: **Database cannot be upgraded because it is read-only, has read-only files or the user does not have permissions to modify some of the files.**

- i. Verify all of the MUSE databases are listed in **SQL Server Management Studio**.
- j. Confirm the SQL Server permissions for the MUSE Service users have been met. For more information on these permissions, see [Chapter 3 “MUSE Service Users” on page 41](#).
4. Verify SQL Server logins and roles for MUSE administrator and MUSE background users.

The hospital MUSE and IT Administrators are responsible for ensuring the MUSE Service Users have appropriate SQL Server Logins and Roles. Confirm that the user accounts used for the MUSE system meet the requirements specified in [“SQL Server Role Requirements” on page 43](#).

## Updating the MUSE Database Server Configuration

After moving the MUSE databases, the MUSE installed configuration needs to be modified to point to the new database server. Perform the following steps on the MUSE application server and any MUSE client or modem servers that have the MUSE Modem feature installed:

1. Log on to Windows:

Point of Access	Log on as
MUSE Application Server	MUSE Administrator user
MUSE Client Workstation	Local administrator

2. Go to **Control Panel > Programs and Features**.
3. Select **MUSE 9** and click **Change**.  
The **Welcome ...** window opens.
4. Select **Modify** and click **Next**.  
The **Select Features** window opens.
5. Click **Next**.
6. If the prompt, **SQL server 2008 or SQL server 2008 R2 or SQL server 2012 or SQL server 2014 is not installed. This warning can be ignored if you are installing the MUSE database on a different machine. Do you want to continue?**, opens, click **Yes**.  
The **MUSE Client Configuration** window opens.

7. Click **Next**.

The **Select Database Server** window opens.

8. Click **Browse** or type the name of the SQL Server where the MUSE databases are located.

Be sure to include the instance name if a non-default SQL Server instance will be used.

Default instance example: **SQLSERVER**

Named instance example: **SQLSERVER\INSTANCE**

**NOTE:**

You must specify the SQL Server by name. Do not use the IP Address of the SQL Server.

9. Click **Next**.

If the following prompt opens: **The database being selected must be at the same version as the MUSE Server software. Do you want to proceed?**, click **Yes**.

The installer validates that the database is available. If the database cannot be found, the following SQL Server Validation warning message is displayed:

**Database not found, please manually verify that the database server is correct. Once the database server is available the MUSE Services installed on this box must be restarted. Do you want to continue?**

10. Click **No**.

Verify the name and instance of the SQL Server before proceeding.

11. If the database validation is successful, the **MUSE Services Configuration** window opens.

12. Confirm the correct **MUSE Background User Name**, **Password**, and **MUSE Administrator User Name** are populated in the fields of the **Services Configuration** window.

**NOTE:**

The **MUSE Administrator User** field is not present when modifying the MUSE configuration on a MUSE client

13. If these user names and passwords do not need to be changed, skip to the next step. If these user name and passwords need to be changed, perform the following steps:

- a. Type the user name and password for the **MUSE Background** account and the user name for the **MUSE Administrator**.

- If you are using a domain account, type the user name in **<domain name>\<user name>** format
- If you are using a local account, type the user name in **.\<user name>** format
- No password is required for the MUSE Administrator user account.

- b. The MUSE installer installs the MUSE Services using the **MUSE Background** account and password that you entered here. When you perform these steps on the MUSE application server, the MUSE installer also populates



the **MUSE Background** and **MUSE Administrator** accounts in the MUSE database with these same Windows user names and password.

- c. Use the **Advanced Options** button to specify **Service Command Line Arguments**.

Do not use this button unless specifically directed to do so by MUSE Engineering or MUSE Technical Support.

14. Click **Next**.

The installer validates that the user accounts you selected do exist on the system.

If you receive a warning message that the account was not found or user validation failed, click **No** at the prompt to return to the **Services Configuration** window and check the following:

- The user names for the accounts and the password are correct.
- The accounts exists.

The **Choose MUSE Options** window opens.

15. Click **Next** until the **Maintenance Complete** window opens.
16. Click **Finish**.

### Canceling the Auto Shutdown

Perform the following steps to cancel the Auto Shutdown and ensure that MUSE services are started.

1. Cancel the MUSE shutdown using the instruction in [“Canceling the System Shutdown” on page 59](#).
2. Verify all MUSE services have started.

### Re-install MUSE API 3.1

Since the database server was changed as part of modifying the MUSE installation, MUSE API 3.1 needs to be re-installed.

If the MUSE API3 service is not installed, you do not have to do this.

For information on how to uninstall and re-install MUSE API 3.1, refer to the *MUSE v9 Cardiology Information System Devices and Interfaces Manual*.

## Renaming the MUSE Systems

This section describes the processes and steps necessary to rename the MUSE application server, MUSE HL7 Interface (CCG), and MUSE Client.

### Renaming the MUSE Application Server

If the computer name of the MUSE application server needs to be changed after the MUSE software has already been installed, use the following procedure to change the computer name. Renaming the MUSE file server can require the assistance and

cooperation of the local IT department. Renaming the MUSE application server consists of the following steps:

1. Shutting down the MUSE services.
2. Renaming the MUSE application server.
3. Updating the SQL Server configuration (local databases only).
4. Updating the MUSE configuration.
5. Canceling the Auto Shutdown.
6. Re-installing MUSE API 3.1.

The following items are additional conditional considerations that you should review when you rename the MUSE application server:

- If MUSE Web Compatibility Layer is installed on the application server, any users or systems (such as CASE) using the MUSE Web URL by name need to be updated with the new name.
- If CV Web 3 is installed on the server, any users or systems using the CV Web 3 URL by name need to be updated with the new name.
- If any systems (such as CASE) are accessing the MUSE application by name, those systems need to be updated with the new name.
- If the MUSE application server is hosting any MUSE modems or printers, the computer name for the modem and/or printer in the MUSE system must be updated with the new name.

## Shutting Down MUSE Services

Perform the following steps to shut down the MUSE services.

1. Log on to the MUSE application server as the MUSE Administrator user.
2. Perform a full shutdown of the MUSE system using the instructions in [“Auto Shutdown” on page 57](#).

Notify all users that the system is being shut down for maintenance.

3. After the Auto Shutdown is complete, stop all MUSE services on the MUSE application server.
4. Set the MUSE service **Startup Type** to **Manual**.

This step prevents any MUSE services starting if the system is rebooted.

## Renaming the MUSE Application Server

Perform the following steps to rename the MUSE application server.

1. Ask the local IT or network administrator to change the computer name of the MUSE application server.
2. Reboot the MUSE application server.
3. Confirm that the server name has been changed and that the server is still a member of the domain.

## Updating the SQL Server Configuration

Perform the following steps to update the SQL Server configuration.

These steps should only be performed if the database is local to the MUSE application server. If the SQL Server database is remote, proceed to [“Updating the MUSE Configuration” on page 67](#).

1. Log on to the MUSE application server as a Windows user that has the sysadmin server role on the SQL Server.
2. Open **SQL Server Management Studio** and connect to the server using the new computer name.
3. Create and execute the following query:
 

```

      --- BEGIN QUERY ---
      EXEC SP_DROPSEVER 'OLDSEVER'
      EXEC SP_ADDSEVER 'NEWSEVER', local
      --- END QUERY---
```

Where **OLDNAME** is the old computer name and **NEWNAME** is the new computer name.
4. Verify the message, **Command(s) completed successfully**, opens in the **Messages** tab.
5. Close **SQL Server Management Studio**.
6. Restart the SQL Server (**MSSQLSERVER**) service.
7. Open **SQL Server Management Studio** and connect to the server using the new computer name.
8. Create and execute the following query:
 

```

      --- BEGIN QUERY ---
      SELECT @@SERVERNAME as 'Server Name';
      --- END QUERY ---
```
9. Verify that the **Results** tab shows the new computer name as the value for **Server Name**.
10. Close **SQL Server Management Studio**.

## Updating the MUSE Configuration

After renaming the server, the MUSE installed configuration needs to be modified to point to the new application server. These steps need to be performed on the MUSE application server and all MUSE clients.

1. Log on to Windows:

Point of Access	Log on as
MUSE Application Server	MUSE Administrator user
MUSE Client Workstation	Local administrator

2. Go to **Control Panel > Programs and Features**.
  3. Select **MUSE 9** and click **Change**.
- The **Welcome ...** window opens.

4. Select **Modify** and click **Next**.  
The **Select Features** window opens.
5. Click **Next**.
6. If the prompt, **SQL server 2008 or SQL server 2008 R2 or SQL server 2012 or SQL server 2014 is not installed. This warning can be ignored if you are installing the MUSE database on a different machine. Do you want to continue?**, opens, click **Yes**.  
The **MUSE Client Configuration** window opens.  
If these steps are being performed on the MUSE application server, the **Server Name** is greyed out and pre-filled with the new name of the server. If these steps are being performed on a MUSE client, manually type in the new computer name of the MUSE application server.
7. Click **Next**.  
If a confirmation prompt opens to confirm the new name of the server, click **Yes**.
8. Perform one of the following:
  - If the **Select Database Server** window opens, proceed to step 9.
  - If the **Maintenance Complete** window opens, proceed to step 17.
9. Click **Browse** or type the name of the SQL Server where the MUSE databases will be or are installed.  
Be sure to include the instance name if a non-default SQL Server instance will be used.  
Default instance example: **SQLSERVER**  
Named instance example: **SQLSERVER\INSTANCE**  
**NOTE:**  
You must specify the SQL Server by name or **(local)**, do not use the IP Address of the SQL Server.
10. Click **Next**.  
If the following prompt opens: **The database being selected must be at the same version as the MUSE Server software. Do you want to proceed?**, click **Yes**.  
The installer validates that the database is available. If the database cannot be found, the following SQL Server Validation warning message is displayed: **Database not found, please manually verify that the database server is correct. Once the database server is available the MUSE Services installed on this box must be restarted. Do you want to continue?**
11. Click **No**.  
Verify the name and instance of the SQL Server before proceeding.
12. If the database validation is successful, the **MUSE Service Configuration** window opens.

13. Confirm the correct **MUSE Background User Name, Password**, and **MUSE Administrator User Name** are populated in the fields of the **Services Configuration** window.

**NOTE:**

The **MUSE Administrator User** field is not present when modifying the MUSE configuration on a MUSE client

14. If these user names and passwords do not need to be changed, skip to the next step. If these user name and passwords need to be changed, perform the following steps:
  - a. Type the user name and password for the **MUSE Background** account and the user name for the **MUSE Administrator**.
    - If you are using a domain account, type the user name in **<domain name>\<user name>** format
    - If you are using a local account, type the name user name in **.\<user name>** format
    - No password is required for the MUSE Administrator user account.
  - b. The MUSE installer installs the MUSE Services using the **MUSE Background** account and password that you entered here. When you perform these steps on the MUSE application server, the MUSE installer also populates the **MUSE Background** and **MUSE Administrator** accounts in the MUSE database with these same Windows user names and password.
  - c. Use the **Advanced Options** button to specify Service Command Line Arguments.  
  
Do not use this button unless specifically directed to do so by MUSE Engineering or MUSE Technical Support.
15. Click **Next**.  
  
The installer validates that the user accounts you chose exist on the system.  
  
If you receive a warning message that the account was not found or user validation failed, click **No** at the prompt to return to the **Services Configuration** window and check the following:
  - The user names for the accounts and the password are correct.
  - The accounts exists.

The **Choose MUSE Options** window opens.
16. Click **Next** until the **Maintenance Complete** window opens.
17. Click **Finish**.

### Canceling the Auto Shutdown

Perform the following steps to cancel the Auto Shutdown and ensure that MUSE services are started.

1. Cancel the MUSE shut down following the procedures in [“Canceling the System Shutdown” on page 59](#).
2. Verify all MUSE services have started.

## Re-Installing MUSE API 3.1

Since the database server may have been changed as part of modifying the MUSE installation, MUSE API 3.1 may need to be re-installed.

If the MUSEAPI3 service is not installed or the database server is remote and did not change, you do not have to do this.

For information on how to uninstall and re-install MUSE API 3.1, refer to the *MUSE v9 Cardiology Information System Devices and Interfaces Manual*.

## Renaming the MUSE HL7 Interface (CCG Server)

To rename a MUSE HL7 Interface, have the local IT or network administrator complete the following steps:

1. Rename and restart the server.
2. Verify the name change and that the computer has joined the domain.

If the Test MUSE HL7 Interface also has the MUSE software installed on it, also use [“Renaming the MUSE Application Server” on page 65](#).

## Renaming the MUSE Client

To rename a MUSE client, have the local IT or network administrator complete the following steps.

1. Rename and restart the client.
2. Verify the name change and that the computer has joined the domain.

If the MUSE client is hosting any MUSE modems or printers, the computer name for the modem and/or printer in MUSE must be updated with the new name.

## Changing the MUSE Port Number

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. This section provides instruction to

- Change the port number on the MUSE server
- Change the port number on a MUSE client.

### 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 Application Server

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

1. Log on to the MUSE application server as MUSE Administrator.
2. Perform a system shutdown. For instructions to perform a system shutdown, see [“Activating System Auto Shutdown” on page 58](#).
3. Go to **Control Panel > Programs and Features**.

4. Select **MUSE 9.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. Type the **port number** you want to use and Click **Next**.
8. Click **Next** on the remaining windows to save your change.
9. On the **Maintenance Complete** window, click **Finish**.  
The MUSE services restart.
10. After the change is complete, cancel the **AutoShutdown** using the instructions in ["Canceling the System Shutdown" on page 59](#).

### Changing the Port Number on the MUSE Clients

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

1. Log on to the MUSE client as an administrator user.
2. Go to **Control Panel > Programs and Features**.
3. Select **MUSE 9** and click **Change**.
4. Click **Next** until the **MUSE Client Configuration** window opens.
5. Verify the correct **Server Name** and **Port** are entered and click **Next**.  
If the following message and/or prompt is displayed, **MUSE server not found** and/or **Port validation failed**, proceed to step 6, otherwise proceed to step 7.
6. The **MUSE server not found** and/or **Port validation failed** messages indicate that the MUSE application server could not be found and/or the selected port could not be validated. Both of these messages typically occur regardless of whether just the MUSE server name cannot be found, the port cannot be validated, or both.  
Perform the following steps:
  - a. Click **OK** to the **MUSE server not found** prompt and **No** to the **Port validation failed** prompt.
  - b. Return to step 5.
7. Click **Next** on the remaining windows to save your change.
8. On the **Maintenance Complete** window, click **Finish**.





# Maintenance

GE Healthcare no longer supplies hardware with MUSE systems. Some hardware previously supplied with legacy MUSE systems is compatible with the MUSE v9 system. This manual does not contain any information on GE Healthcare supplied hardware, including repair and maintenance procedures. For hardware supplied with legacy versions of the MUSE system, refer to the appropriate legacy MUSE Service Manual.

**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.

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

## OEM Maintenance

For information on maintenance of Original Equipment Manufacturer (OEM) components, refer to the appropriate OEM manuals for the recommended maintenance of their product.

## Safe Shutdown Procedures

This section provides safe shutdown procedures for the MUSE application server, the MUSE database server, the MUSE HL7 interface (CCG), and the MUSE client.

### Shutting Down the MUSE Application Server

Use the following instructions to safely shut down the MUSE application server.

1. Before shutting down the server, notify all users of the scheduled shutdown.
2. Perform a full or partial shutdown at the MUSE server.  
[See “Auto Shutdown” on page 57.](#)
3. After the MUSE application is shut down, shut down the server following normal Windows shutdown procedures.
4. After restarting the server, cancel the Auto Shutdown.  
[See “Canceling the System Shutdown” on page 59.](#)

## Shutting Down the MUSE Remote Database Server

Prior to shutting down or rebooting the MUSE remote database server, perform a shutdown of the MUSE application server using the steps in [“Shutting Down the MUSE Application Server”](#) on page 73.

## Shutting Down the MUSE HL7 Interface (CCG)

Use these instructions to safely shut down the MUSE HL7 interface.

1. From the Windows desktop, open **IDE interface** and manually stop the threads and processes for any active Cloverleaf sites (usually ***muse\_prod*** and ***his\_prod***).

**NOTE:**

Due to the variance in the existing sites, threads, and processes for a given Cloverleaf implementation with MUSE, specific thread and process names cannot be provided here. Contact GE Healthcare technical support for specific assistance with determining thread and process names.

2. Stop the ***Infor Cloverleaf(R) Integration Services 60*** service.
3. Shut down the system following normal Windows shutdown procedures.

## Shutting Down the MUSE Client

Use the following instructions to safely shut down the 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.

## 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.

**NOTE:**

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

Checkout procedures are separated into two categories:

- [“Hardware FRU Repairs”](#)
- [“Non-FRU Repairs”](#)

Follow the checkout procedure appropriate for the repair you performed.

## Hardware FRU Repairs

This manual does not contain any information on GE Healthcare-supplied hardware, or repair and maintenance procedures. For hardware supplied with legacy versions of the MUSE system, refer to the appropriate legacy MUSE service manual.

## 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.

### Inbound Device Checkouts

Use the following procedures to verify that inbound devices are working correctly.

#### Modem Feature (CSI Modem, CSI Network, CSI Direct)

1. Transmit a test from a device that uses the MUSE Modem feature.
2. Verify that the test is acquired into the MUSE system.

#### DCP Inbound

1. Transmit a test from a device that uses the DCP.
2. Verify that the test is acquired into the MUSE system.

#### Share Folder/Generacq (MARS, CASE/CS, Monitoring Gateway, eDOC Connect)

1. Transmit a test from a device to a Share Folder defined in the MUSE system.
2. Verify that the test is acquired into the MUSE system.

#### XML Inbound

1. Transmit a test in MUSE XML format from a device to the XML folder on the MUSE system
2. Verify that the test is acquired into the MUSE system.

### Output Device Checkout

Use the following procedure to verify that outbound devices are working correctly.

1. Use the Print Test function of MUSE to manually send a test to an outbound device defined in MUSE.
2. Verify that the outbound device received the output from the MUSE system.
3. Verify the format of the output matches the format setting used as appropriate.

### Report Distribution Checkout

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

1. Determine the report distribution configuration for a location that needs to be checked out.
2. Acquire, demographics complete, or confirm data for the location determined in step 1 as appropriate.
3. Verify the output device(s) setup in the report distribution for the location of the report received the output from the MUSE system.

## 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.

## User Setup

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

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

## 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 v9 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 on as a user who has access to CV 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 InSite ExC.
2. Confirm that you can access the customer's desktop via the remote connection.

## 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 Log**.
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 Log**.
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.

## Logon

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.

### LDAP Authentication

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

### Windows + LDAP Authentication

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

## Discarding, Recovering, and 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**.

## DICOM Checkouts

Use the following procedures to verify that DICOM features are working correctly.

### Receiving DICOM Tests into the MUSE System

1. Send a DICOM test from a DICOM Storage Service Class User device into the MUSE system.
2. Verify that the test is acquired into the MUSE system.

### Sending DICOM Tests from the MUSE System

1. Use the Print Test function of MUSE to manually send a test to an outbound DICOM IOD or PDF device defined in MUSE.
2. Verify that the test is transmitted from the MUSE system to the receiving DICOM system.

### Querying for DICOM Orders

Verify orders from the DICOM Modality Worklist Service Class Provider are visible in the MUSE system.

## Optional Hardware Accessories for MUSE

This MUSE v9 service manual only references the optional hardware shipping with the MUSE v9 system at the time of its release.

### MultiTech MT9324ZBA Modem

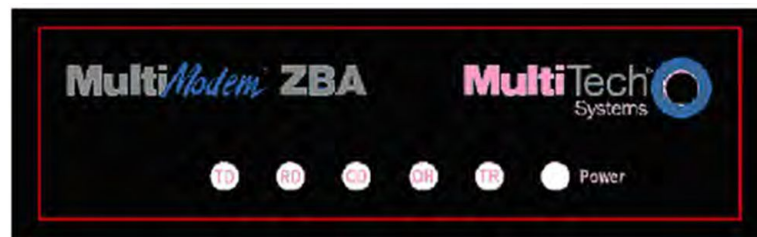
Modems are used to transmit patient ECGs from the ECG Cart to the MUSE server. For additional information on a modem other than the MultiTech MT9324ZBA, go to the MultiTech Web site to see the appropriate user guide for the modem.

MultiTech Modem Drivers can be found on the MUSE v9 support disc. Instructions for installing the modem drivers are located in the MultiTech Modem MT9234ZBA Driver Installation documentation.

For specifications for the MultiTech MT9324ZBA modem, see the MultiTech Web site.

### LED Connectors

The LED indicators on the front panel indicate status, configuration, and activity.



LED Indicator Name	Description
TD – Transmit Data	Flashes when the modem is transmitting data to another modem.
RD – Receive Data	Flashes when the modem is receiving data.
CD – Carrier Detect	Lights when the modem detects a valid carrier signal from another modem. It is on when the modem is communicating with the other modem and off when there is no connection.
OH – Off-Hook	Lights when the modem is off-hook, which occurs when the modem is dialing, online, or answering a call.

TR – Terminal Ready	Lights when a communication program is using the modem. It means the modem is ready for an outgoing or incoming call. It goes off when the communication program disconnects the serial port. When it goes off, a connected modem also disconnects.
Power	Lights when the system is applying power to the modem.

### Replacement Parts

GE Part Number	Description
2003097-001	Fax/CSI/Xmodem Modem Kit 120V
2003097-002	Fax/CSI/Xmodem Modem Kit 220V

### Barcode Reader

GE Healthcare purchased the barcode readers that can be used with your system from the original equipment manufacturer (OEM). Due to the constant changes in design and specifications, refer to the OEM Web sites for additional information not located in this manual

#### Hand Held 3800G Barcode Reader

For barcode specifications, refer to the user's guide found at the OEM Web site.

The following parts are available.

GE Part Number	OEM Part Number	Description
2038834-001	3800G04-USBKITE or HHP-1300G-2USB	BARCODE SCANNER, HANDHELD, USB
2040065-001	42206132-02E	BARCODE SCANNER 3800G PS/2 CABLE

#### Hand Held Flexpoint HS-1M Barcode Reader

For barcode specifications, refer to the user's guide found at the OEM web site.

All replacement parts are provided by Jadak. See the Jadaktech Web site.



# Disaster Recovery

## MUSE System Backup and Recovery

A backup and recovery plan is crucial to prevent data loss and to minimize service interruption in the event of system failure or disaster. All MUSE v9 installations are software-only, customer-supplied hardware configurations. With the release of the MUSE v9 application, previous tape and network backup configurations utilized in GE Healthcare-supplied hardware configurations are no longer documented or supported.

It is the customer's responsibility to configure and monitor backup and disaster recovery procedures and to execute those procedures as necessary. GE Healthcare is not liable for any loss of data, your inability to access data, any failure of system performance, or any claims that would otherwise potentially be covered by your warranty, if any such problem results from, or arises out of, your selected backup or disaster recovery procedures. GE Healthcare service representatives may still be able to assist you in correcting such a problem, on a billable basis.

## Windows Operating System and SQL Server

Backing up the Microsoft Windows operating system and SQL Server is the responsibility of the customer.

Customer must decide if they want to perform backups of the Windows operating system and SQL Server in the case of disaster recovery.

## MUSE System Software

Backing up MUSE system software and configuration is the responsibility of the customer.

The MUSE application and MUSE related software can be re-installed in the case of a disaster recovery situation. The core MUSE software is as follows:

- MUSE application
- MUSE API 3
- MUSE Web Compatibility Layer and Web site(s)
- InSite ExC

Extra steps can be taken to backup the configuration files for each of these items to aid in restoration in a disaster recovery situation. The following list provides the file, file description, and default location for each MUSE software component.

MUSE Software	File, File Description, and Default Location
MUSE application	<b>File:</b> <i>server.remoting.config</i> <b>Description:</b> Contains the MUSE port information for the MUSE server; default is 8001. <b>Default Location:</b> <i>C:\Program Files (x86)\MUSE</i>
MUSE API 3	<b>File:</b> <i>MUSEAPIService.exe.config</i> <b>Description:</b> Contains the MUSE API Service / port configuration. <b>Default Location:</b> <i>C:\Program Files (x86)\MUSE</i>
MUSE Web Compatibility Layer <sup>1</sup>	<b>File:</b> <i>web.config</i> <b>Description:</b> Contains the MUSE Web Compatibility Layer Web site configuration information. <b>Default Location:</b> <i>C:\inetpub\wwwroot\MUSEWebCompatibilityLayer</i> <sup>1</sup> If additional MUSE Web Compatibility Layer Web sites were installed, additional folders are created in c:\inetpub\wwwroot and need to also have their configurations saved.
InSite ExC	Use the instructions in the InSite ExC Installation document to back up the InSite ExC configuration to a file.

## MUSE Database Backup

MUSE database backup is the responsibility of the customer.

The MUSE databases must be backed up on a regular basis; the frequency and recovery model is up to the customer.

MUSE databases use the **SIMPLE** recovery model by default. This means that you can restore from your last backup. Any data changes since the last backup are lost. If you want more protection, you can modify the SQL database recovery model.

Knowledge of the MUSE database helps you understand the backup requirements. The MUSE system uses the SQL Server 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 exist: for example, **MUSE\_Site0002**, **MUSE\_Site0003**, and so on.

## MUSE Database Restoration

MUSE database restoration is the responsibility of the customer.

Follow Microsoft's instructions for restoring a SQL Server backup using **SQL Server Management Studio** or other restoration method used by your facility.

To ensure data integrity, it is crucial that you back up or restore all databases together. Backing up or restoring individual databases could result in data mismatches, database errors, or data corruption.

For example, do not restore **MUSE\_Site0001** without also restoring **MUSE\_System**, **MUSE\_SiteTemplate**, and any other **MUSE\_SiteXXXX** databases that are part of the MUSE system.

## MUSE Application Server Disaster Recovery

MUSE application server disaster recovery is the responsibility of the customer.

System rebuild and replacement, including operating system and SQL Server installation, must be completed before GE Healthcare service personnel can aid in re-installing MUSE software.

The following are the high-level steps to restore the MUSE Application Server in the event of a complete system failure.

1. Install physical server.
2. Install operating system and SQL Server.
3. Restore MUSE databases.
4. Install MUSE system software.
5. Restore MUSE system software configuration(s).
6. Reconnect MUSE clients.
7. Reconnect device(s) such as MARS, CASE, MAC carts, as necessary.

Refer to the appropriate MUSE documentation for the installation of the MUSE system software, clients, and devices.

## MUSE HL7 Interface (CCG) 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.

## MUSE HL7 Interface (CCG) Configuration Backup and Restoration

GE Healthcare configures a weekly backup of the HL7 configuration as a Windows scheduled task called **System\_State\_Recurring\_Backup**. This scheduled task saves the configuration to the **SystemState** folder of the drive where the CCG software is installed.

The customer is responsible for making a copy of this folder and saving it to a network drive or external media.

The GE Healthcare HL7 engineer performs the configuration restoration .

## MUSE HL7 Interface (CCG) Disaster Recovery

The following are the high-level steps to restore the MUSE HL7 Interface (CCG) in the event of a complete system failure.

1. Install server.
2. Install operating system.
3. Install MUSE HL7 interface (CCG) software.
4. Restore MUSE HL7 interface (CCG) software configuration(s).
5. Reconnect to MUSE application server.

Refer to the *MUSE v9 Cardiology Information System Centricity Clinical Gateway (CCG) Installation Manual* for instructions to install the MUSE HL7 Interface (CCG) software.

## MUSE Test System Disaster Recovery

MUSE test systems have the same expectations and follow the same system backup and restore, database backup and recovery, and HL7 configuration backup and recovery as production systems. In some cases, SQL Server and MUSE HL7 interface software can be installed on the same test system.

See the appropriate section above for appropriate information.

## MUSE Client Disaster Recovery

MUSE clients can be rebuilt from scratch in a disaster recovery situation. The following are the high-level steps to restore the MUSE HL7 Interface (CCG) in the event of a complete system failure

1. Install physical workstation.
2. Install operating system.
3. Install MUSE application software.
4. Reconnect to MUSE application server.

Refer to the appropriate MUSE documentation for the installation of the MUSE application software.

**NOTE:**

Some client hardware previously supplied with legacy MUSE systems may be compatible with MUSE v9. This manual does not contain any GE Healthcare supplied hardware information, repair, or maintenance procedures. For hardware supplied with legacy versions of the MUSE system, refer to the appropriate MUSE legacy service manual.



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

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 and 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 88](#) or [“Updating Legacy System Data” on page 88](#).

## 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

Position	Factor
4	7
5	6
6	5
7	4
8	3
9	2

- Add the results of each multiplication together.
- Divide the total by 11 and establish the remainder.
- 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.
- 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 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 and 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:

A database search allows the user to input PID, but requires the user to enter the exact format. The format is 3 3 4, for example, *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 dash (—) character (used as a separator) with the character in the database.

# Installing the NHS Number Feature

The NHS Number Feature can be enabled during initial MUSE database installation or manually by changing the customer ID of the system.

## Enable NHS Number during Initial MUSE Database Installation

The NHS Number feature is enabled by selecting a **Customer value** of **NHSNUMBER** during the installation of a new MUSE database. Refer to the *MUSE v9 Cardiology Information System Installation and Upgrade Manual* for information on installing the MUSE database and selecting the **Customer value** during the installation.

The MUSE installer cannot be used to change the Customer after the database has only been installed; it can only be used during the creation of a new database.

## Enable NHS Number by Manually Changing the Customer ID of the System

1. Log on to the MUSE system as MUSE Administrator.
2. Perform a system shutdown.  
For instructions to perform system shutdown, see [“Activating System Auto Shutdown” on page 58](#).
3. Using **SQL Server Management Studio**, log on to the SQL Server instance where the MUSE databases reside.
4. Open **New Query** and execute the following query:

```
update MUSE_System.dbo.cfgSystem set CustomerID=17
```

The command returns a series of results as **(1 row updated)**.

5. Cancel the AutoShutdown using the instructions in [“Canceling the System Shutdown” on page 59](#).
6. From the MUSE application, go to **System>Setup**.
7. Open **System Properties** and verify the **CustomerID** is 17.

# Updating Legacy System Data

## Utility

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 is called **NHSNumberUpdate.exe** and is located in the **NHS Number Update** folder on the MUSE Support media.



The utility sets the various PIDs in the proper format and adds a verification status. The following list details the order that verification status occurs.

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.

## Application

Since updating the data is a potentially long running process, an application was created to display the update status as the data is converted.

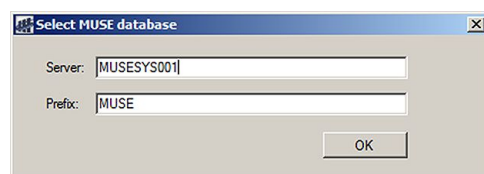
1. Log on to the MUSE application server as MUSE Administrator.
2. Perform a full system shutdown.
 

For instructions to perform system shutdown, see [“Activating System Auto Shutdown” on page 58](#).
3. Insert or mount the MUSE v9 Support media into the optical drive.
4. Copy **\NHS Number Update\NHSNumberUpdate.exe** from the MUSE v9 Support media to the location where the MUSE application is installed.

Default is **C:\Program Files (x86)\MUSE**.

5. Execute **NHSNumberUpdate.exe** from the MUSE application installation folder.
 

The **Select MUSE database** window opens.



6. In the **Server** field, type the name of the MUSE database server where the MUSE databases reside.

If the databases are installed in a default instance, only the name of the SQL Server is required. If the databases are located on a named instance of SQL Server, include the instance name. For example, if the databases are located on **SQLSERVER1** in a named instance called **MUSE**, type **SQLSERVER1\MUSE**.

7. The **Prefix** field defaults to **MUSE**.

Leave this at default and do not change it unless instructed by Technical Support or Engineering.

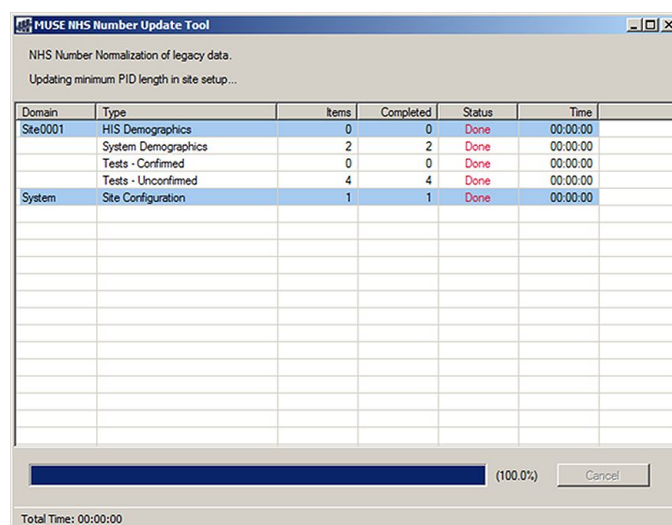
8. Click **OK**.

One of the following occurs:

- If the NHS Number feature is enabled, the **MUSE NHS Number Update Tool** appears.
- If the NHS Number feature is not enabled on the MUSE system the following message is displayed: **The NHS Number feature is not currently installed on the MUSE System, so the utility cannot run.**

Click **OK**. Close the tool and enable the NHS Number feature using [“Enable NHS Number during Initial MUSE Database Installation”](#) on page 88.

9. Click **Start** to begin the conversion process.



A progress bar fills as the conversion executes. When the progress bar is 100%, the conversion is complete. The screen displays the total number of items processed, the total number of completed items, and the status of each process. The NHS Number Update Tool log file is **C:\ProgramData\MUSE\MUSE\_NHSNumberUpdate.log**.

- When the conversion is complete, the tool can be closed.
- Cancel the AutoShutdown using the instructions in [“Canceling the System Shutdown”](#) on page 59.



# MUSE Database Language Change Tool

Use the following procedures to install, run, and verify the MUSE Database Language Change Tool.

## Installing the Database Language Change Tool

Use the following instructions to install the MUSE Database Language Change Tool on to the MUSE server:

1. Log on to the MUSE server as a user with administrator rights.
2. On the MUSE Support CD, navigate to the **MUSEDLanguageChanger** directory.
3. Copy the file **MUSEDLanguageChanger.exe** into the MUSE installation folder.

## Running the Database Language Change Tool

Use the following instructions to change the MUSE database language.

1. Log on to the MUSE application server as MUSE Administrator.
2. Shut down the MUSE application using the Full AutoShutdown instructions.  
For instructions for AutoShutdown, see [“Auto Shutdown” on page 57](#).
3. Run **MUSEDLanguageChanger.exe** from the MUSE installation folder.  
The **MUSE Database Language Change Tool** opens.
4. Enter the settings needed to change the MUSE database language.
  - a. Type the name of the server where the database is located.  
Use the default value (**local**) if the database is located on the same computer from which you are executing the **MUSE Database Language Change Tool**.

For databases in a named instance, use the format **ServerName\InstanceName**.

- b. Type the prefix for the MUSE database, if it is different from the default (**MUSE**).
  - c. Select the new language and indicate if the ECG statements should be in English.
5. Click **Start** to start the database language conversion.

The Database Language Change Tool log file is **C:\ProgramData\MUSE\MUSEDLanguageChanger.log**.

When the conversion completes, a completion dialog box opens.

**NOTE:**

The conversion time is dependent on the number of sites and may be lengthy if the system has a large number of MUSE sites.

6. Click **OK** to close the completion dialog box.
7. Click **Exit** to close the **MUSE Database Language Change Tool**.
8. Cancel the MUSE shutdown using the instructions in [“Canceling the System Shutdown” on page 59](#).

## Verifying the Database Language Change

Use the following instructions to verify that the language change was successful.

1. From the MUSE application, go to **System > Setup**.
2. Open System Properties and verify the two-letter **Database Language** value matches the expected database language.
3. To identify the statement library language, go to the Statement Library within MUSE setup and verify the language of the existing statements.



# Configuring MUSE System for LDAP Authentication

The following is an overview of the process to configure the MUSE system for LDAP Authentication:

1. Customer works with GE Healthcare to understand the requirements, features, and limitations of LDAP Authentication and to ensure that this authentication method meets their needs.
2. Install the LDAP Authentication feature option in MUSE.
3. Configure LDAP in the MUSE system.

The following table details some of the requirements, features, and limitations of using LDAP with the MUSE system. Both GE Healthcare personnel and customer personnel can use the following table to determine if LDAP Authentication meets the customer's expectations.

Requirements	<ul style="list-style-type: none"> <li>Microsoft Active Directory Server <b>givenname</b> and <b>sn</b> fields must be populated in the LDAP server's user schema for every user that uses LDAP authentication in MUSE. If the <b>givenname</b> or <b>sn</b> field is blank for a given LDAP user, the blank field(s) can prevent the user logging on to MUSE using LDAP authentication.</li> <li>For Microsoft Active Directory, <b>givenname</b> is the same as First Name and <b>sn</b> is the same as Last Name (surname).</li> </ul>
Features	<ul style="list-style-type: none"> <li>Allows users to log on to MUSE with a domain / active directory user and password. LDAP authentication can be combined with Windows authentication.</li> <li>Provides more centralized administration of MUSE users, roles, and profiles.</li> <li>Provides mapping of LDAP groups to MUSE Roles and Profiles.</li> <li>Provides mapping of LDAP fields to MUSE fields.</li> <li>Automatically creates MUSE users from LDAP users.</li> <li>Can automatically enable MUSE users who have been created from LDAP users.</li> <li>Allows site overrides in the MUSE user setup to override LDAP group to MUSE role mappings. These overrides can be used to ensure that any specified user is never affected by the LDAP group configuration.</li> </ul>
Limitations	<ul style="list-style-type: none"> <li>Requires manual configuration of job titles within the MUSE User setup.</li> <li>Requires manual configuration of MUSE user access as any MUSE user created by LDAP has access to all sites in the MUSE system.</li> <li>Automatically assigns a system user ID to any user created by LDAP.</li> <li>Requires the MUSE LDAP setup to be refreshed when any changes or additions are made to the LDAP server groups if the groups are to be selectable within the MUSE LDAP group mapping function.</li> <li>The Windows User Name for the MUSE Background user must contain the string <code>MuseBkgnd</code> somewhere in it. For example: <code>MuseBkgnd</code>, <code>XYZMuseBkgnd</code>, <code>MuseBkgndXYZ</code>, or <code>XYZMuseBkgndXYZ</code>.</li> </ul>

## Installing the LDAP Authentication Option in the MUSE System

### NOTE:

**BEFORE YOU BEGIN:** If LDAP/AD authentication is going to be used with MUSE, the Windows User Name for the MUSE Background user must contain the string `MuseBkgnd` somewhere in it. For example: `MuseBkgnd`, `XYZMuseBkgnd`, `MuseBkgndXYZ`, or `XYZMuseBkgndXYZ`.

The LDAP Authentication option must be enabled by a qualified MUSE service person prior to the configuration of LDAP in MUSE. If the option is not already enabled, contact your GE service representative to enable the option.

Use the following procedure to verify whether the LDAP option is already enabled.

1. Log on to the MUSE application server as a user that has at least **View System Setup** and **Manage LDAP Settings** privileges in the MUSE system.
2. Go to **System > Setup**.
3. From **System**, select **System**.
4. Right-click on **MUSE Cardiology Information System**.
5. Verify that **LDAP Configuration** is listed in the navigation menu.  
If it is listed, **LDAP Configuration** is enabled.

## Configuring LDAP in the MUSE System

The following section is an overview of the process to configure LDAP in MUSE. When configuring LDAP for the first time, these steps must be performed in this order. Maintenance of the LDAP Fields and Groups can be performed as needed by the MUSE or LDAP administrator.

1. Configure LDAP in the MUSE system properties.
2. Configure LDAP fields in MUSE setup.
3. Configure LDAP groups in MUSE setup.

### 1. Configuring LDAP in the MUSE System Properties

**NOTE:**

Make sure you do not lock yourself out of the system. You can get locked out as follows:

- If users are currently using Windows Authentication and you enable LDAP before it is fully configured.
- If users are currently using MUSE Authentication and you turn off MUSE Authentication and enable LDAP before it is fully configured.

Make sure you configure LDAP according to the following procedure:

1. Log on to the MUSE system as a user that has the **Manage LDAP Settings** privilege in the MUSE application.
2. Go to **System > Setup**.
3. Select **System**.
4. Right-click on the MUSE entry and select **Properties**.
5. Select **LDAP Configuration**.

6. Use the information in the following table to complete the fields:

Field	Instructions to Complete the Field	Notes
<b>LDAP Server Name</b>	Type the full qualified Windows server name or the IP address of the LDAP server.	If this field is not populated, you cannot enable <b>Allow users to login using LDAP authentication</b> .
<b>Port Number</b>	Type the port number of the Internet Protocol address of the LDAP server.  Click <b>Test Connection</b> to confirm that the MUSE system can connect to the specified LDAP server name and port.	The common port number for LDAP servers is 389. The default port number for LDAP over Secure Sockets Layer (SSL) is 636.  If this field is not populated, you cannot enable <b>Allow users to log on using LDAP authentication</b> .
<b>Distinguished Name Path to Groups</b>	Type the distinguished name path to the LDAP groups that contain the users that need access to the MUSE system.  Click the <b>Download Active Directory Groups</b> button to confirm the MUSE can connect to the LDAP path and download groups.	LDAP objects are referenced by their distinguished name (DN). A DN is a sequence of relative distinguished names (RDN) connected by commas. An RDN is an attribute with an associated value in the form of attribute=value. The MUSE system looks for users at the distinguished name path and additionally looks for users recursively that are below the path structure.  The following is an example of a distinguished names path to groups: <b>OU=MUSE Users, DC=corp,DC=hospital,DC=com</b>  The following example is a distinguished names path to users: <b>CN=Users,DC=corp,DC=hospital,DC=com</b>  <b>NOTE:</b> ADSI Edit can be used to help determine/verify the distinguished name paths. See <a href="#">"ADSI Edit" on page 100</a> .
<b>Distinguished Name Path to Users</b>	Type the distinguished name path to the LDAP users that need access to the MUSE system.  After typing the distinguished name path to the users, click <b>Download User Fields</b> to confirm that the MUSE system can connect to the LDAP path and download user fields.	
<b>Allow users to login using LDAP authentication</b>	Select the check box.	After the LDAP feature is properly setup, select this check box to enable MUSE client workstations to authenticate using LDAP.  If setting up LDAP for the first time, do not select this box until all LDAP Groups have been setup.
<b>LDAP new users added are enabled</b>	Select the check box.	After the LDAP feature is properly setup, select this check box to automatically enable new MUSE users created by LDAP authentication.  If setting up LDAP for the first time, do not select this box until all LDAP Groups have been setup.

7. Click **OK** to save your changes.



## 2. Configuring LDAP Fields in MUSE Setup

LDAP Fields are attributes defined within the LDAP database scheme for a person. The LDAP standard defines a person object which contains the following attributes:

LDAP User Attribute	Description
<i>sn</i>	Surname or last name
<i>givenName</i>	Given name or first name
<i>mail</i>	Email address
<i>facsimileTelephoneNumber</i>	FAX number
<i>telephoneNumber</i>	Telephone number

**NOTE:**

There are dozens of LDAP attributes in Active Directory for user schema. See [http://msdn.microsoft.com/en-us/library/ms683980\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms683980(v=vs.85).aspx).

There are more person attributes in LDAP but these attributes are automatically mapped into MUSE user attributes without any configuration needed. Additional mappings can be created to map attributes such as Medicare Identifier to an attribute in the LDAP person object.

When a user launches or logs into the MUSE workstation, if the user authenticates against the LDAP server, the user is added to the MUSE user database using these field mappings. If the user already exists in the MUSE user database, the fields in the MUSE database are updated using the LDAP attributes.

The following table lists the MUSE User fields, whether they are mapped by default, and what their default LDAP Field Name mapping is, if any. Default mappings cannot be changed.

MUSE Field Name	Default Mapping	LDAP Field Name
<i>LastName</i>	Yes	<i>sn</i>
<i>FirstName</i>	Yes	<i>givenName</i>
<i>EmailAddress</i>	Yes	<i>Mail</i>
<i>FaxNumber</i>	Yes	<i>facsimileTelephoneNumber</i>
<i>Phone</i>	Yes	<i>telephoneNumber</i>
<i>Medicare ID</i>	No	
<i>AuxID1</i>	No	
<i>AuxID2</i>	No	
<i>AuxID3</i>	No	
<i>AuxID4</i>	No	
<i>AuxID5</i>	No	

**NOTE:**

If the default field mappings are blank, it indicates that your LDAP configuration is not valid. Return to the **Configuring LDAP in MUSE System Properties** section to ensure LDAP is properly configured there before proceeding

Use the following steps to add a new LDAP field mapping or modify an existing one:

1. Log on to the MUSE system as a user that has the **Manage LDAP User Field Settings** privilege.
2. Go to **System > Setup**.
3. Select **LDAP Fields**.
4. Perform one of the following actions:
  - To create a new mapping, go to **Action > New**.
  - To modify an existing mapping, right-click the entry and select **Properties**.
5. Under **LDAP Attributes/Properties**, select the **LDAP Field** to map from the drop-down list.
6. Under **MUSE Fields**, select the **MUSE Field** to map from the drop-down list.
7. Click **OK** to save your changes.

### 3. Configuring LDAP Groups in MUSE Setup

When properly configured, the LDAP system settings and user field mappings allow for centralized user administration and application authentication. In order to get application authorization, LDAP Groups need to be mapped to MUSE Roles. Mapping LDAP Groups to MUSE Roles allows the LDAP Administrator to add or remove LDAP users to or from an LDAP group and grant that user the privileges associated to the mapped MUSE role.

Use the following steps to add a new LDAP group mapping or to modify an existing one:

1. Log on to the MUSE system as a user that has the **Manage LDAP User Field Settings** privilege.
2. Go to **System > Setup**.
3. Select **LDAP Groups**.
4. Perform one of the following actions:
  - To create a new mapping, go to **Action > New**.
  - To modify an existing mapping, right-click the entry and select **Properties**.
5. Complete the fields using the information in the following table:

Field	Action	Description
<b>LDAP Group</b>	Select the LDAP group from the drop-down list. These are the groups pointed to in the group's description name portion of the LDAP system settings.	Groups are a quick way of giving users common access to certain features or functionality within an LDAP directory.
<b>Rank</b>	Add the ranking of the group by clicking the up and down arrows or by typing a number into the field.	The rank number is used in the case that an LDAP user exists in more than one LDAP group. This would result in a MUSE user existing in multiple MUSE roles. Since a MUSE user can only exist in a single MUSE role, this rank number (highest number wins) determines which MUSE role the MUSE user is in.  The rank range is 1 to 5000. A best practice would be to use multiples of 100 when setting up ranks for the first time so that additional LDAP groups can be more easily added and ranked at a later time.
<b>MUSE Role</b>	Select the MUSE Role from the drop-down list.	MUSE Roles are created using Roles function of MUSE. Each MUSE Role is made up of MUSE privileges.
<b>MUSE Profile</b>	Select the MUSE Profile from the drop-down list. This is optional.	MUSE Profiles are created using the Profile Manager in MUSE. Profiles specify and manage pre-defined sets of user options across all MUSE applications.

- Click **OK** to save your changes.

## Changes to LDAP Groups

After the initial MUSE LDAP configuration, the expectation is that no changes will be made to the LDAP groups on the LDAP server other than adding or removing users from the LDAP groups that have been mapped in MUSE. If any changes are made to the LDAP groups on the LDAP server, such as renaming groups or moving groups, MUSE LDAP Authentication may stop working.

Furthermore, if the **Download Active Directory Groups** button located in the MUSE LDAP Configuration is clicked, all of the LDAP Groups to MUSE Roles and Profiles mappings will be deleted. This is because if any changes are made to the LDAP group configuration on the LDAP server that would require the Active Directory Groups to be re-downloaded, the MUSE LDAP Groups to MUSE Roles must be re-configured from the beginning. If the **Download Active Directory Groups** button is clicked and confirmed in MUSE, all users using LDAP authentication will no longer be able to access the MUSE system until the LDAP group to MUSE role mappings are re-configured. MUSE and Windows Authentication will continue to work if the appropriate shortcuts for these methods exist on each of the MUSE client workstations.

If changes need to be made to the LDAP configuration that would require re-downloading the LDAP groups from the LDAP server, you need to take the following steps:

1. Schedule an appropriate down time for the MUSE system in order to re-configure LDAP in MUSE,
2. Record the current MUSE LDAP Configuration. One way to record this information is via a **Print Screen** of the LDAP Configuration in MUSE. Any configuration changes made here are also logged to the MUSE **Configuration Change Log**.
3. Record the values of the existing MUSE LDAP Groups configuration. One way to record this information is **Print Screen** or **Print List** of the LDAP Groups in MUSE. The deleted values are also logged to the MUSE **Application Log**.
4. Re-configure LDAP using the steps in ["Configuring LDAP in the MUSE System" on page 95](#).

## ADSI Edit

A Windows feature application called ADSI Edit can be installed on the MUSE application server that can aid in troubleshooting/verifying ADSI/LDAP Users and Groups.

## Installing ADSI Edit

ADSI Edit can be installed by enabling the **AD LDS Snap-Ins and Command-Line Tools** using **Windows Server Manager**.

You can also perform the following procedure to automatically install the required components:

1. Insert or mount the MUSE v9 Support media into the optical drive.
2. Browse to the **Pre Install Scripts** folder on the MUSE v9 Support media.
3. Right-click on **Install\_AD LDS\_Tools.bat** and choose **Run as administrator**.  
The batch file executes and installs any required components
4. Using **Windows Server Manager**, verify that the **AD LDS Snap-Ins and Command-Line Tools** feature has been installed as appropriate for the Windows operating system being used

## Using ADSI Edit

1. Log on to the MUSE application server as a domain user; ideally, this is a domain MUSE Administrator user.
2. Go to **Administrative Tools** and execute **ADSI Edit**.
3. Go to **Action > Connect to ....**
4. Click **OK** to connect to the **Default naming context**.

You can now browse the default naming context and verify AD/LDAP users, groups, and distinguished as needed

5. To determine the distinguished name for an object, right-click on the object and choose **Properties**.

The **distinguishedName** is listed as an **Attribute**.

6. Double-click the entry to view the full value for the **distinguishedName** attribute.





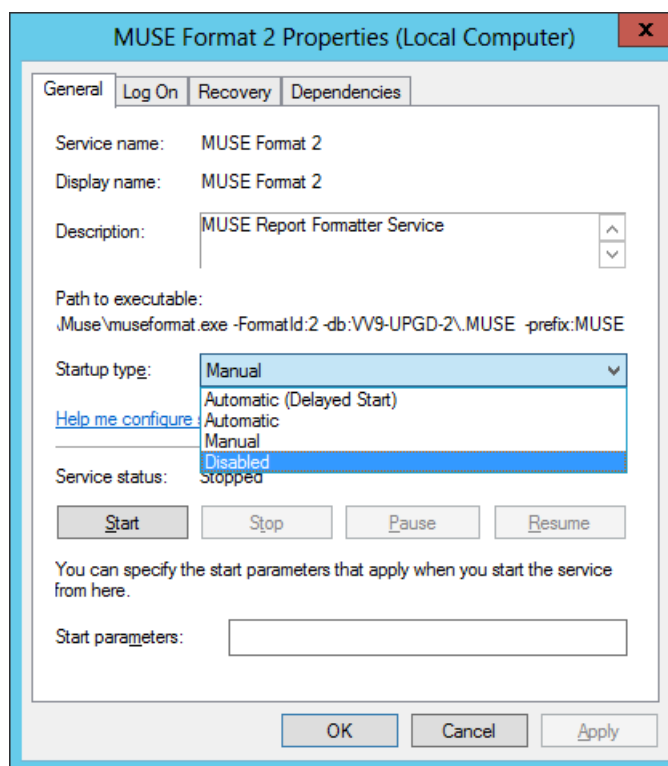
# Support for MARS Holter Reports on MUSE v9 Systems Using Simplified Chinese Language Option

## NOTE:

It is important to implement this configuration on all MUSE V9 systems that are installed with the Chinese Simplified language option.

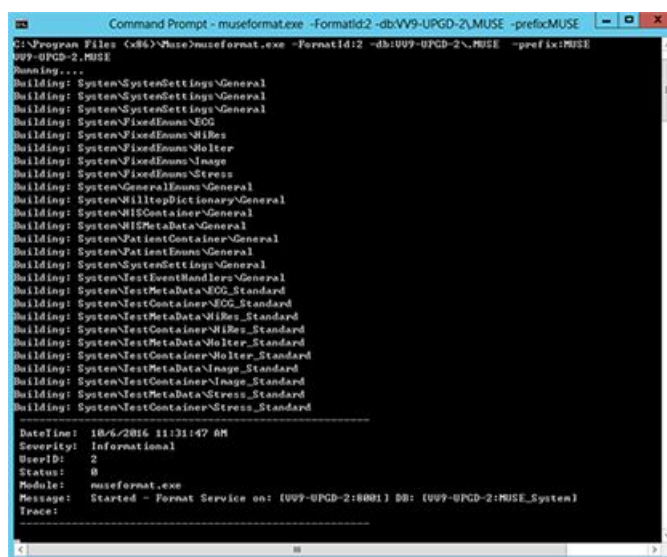
1. Log on to the MUSE application server using the **MUSE Background** account.
2. To disable the **MUSE Format 2** service, use the following steps:
  - a. Go to **Control Panel>Administrative Tools>Services**.
  - b. Right-click **MUSE Format 2** and select **Properties**.

The **MUSE Format 2 Properties (Local Computer)** window opens.



- c. Select **Stop**.  
The **MUSE Format 2** service stops processing.

- d. Under ***Path to executable***, copy and save the command line arguments starting with ***-FormatId:2***.  
  
For example, `-FormatId:2 -db:VV9-UPGD-2\.MUSE -prefix:MUSE`  
  
You will use this path name later in step 3c.
  - e. From the ***Startup type*** menu, select ***Disabled***.
  - f. Click ***OK***.
3. To launch the `museformat.exe` service from the command line, use the following steps:
- a. Launch the Windows ***Command Prompt*** (`cmd.exe`) in administrative mode.  
  
The ***Command Prompt*** window opens.
  - b. Navigate to the MUSE v9 install directory.  
  
For example, `c:\program files (x86)\muse\`
  - c. Enter `museformat.exe` followed by the command line arguments that you copied and saved from the services general properties window  
  
For example, `museformat.exe -FormatId:2 -db:VV9-UPGD-2\.MUSE -prefix:MUSE`
  - d. Press ***Enter*** to launch the service.  
  
Verify that the service has started and that you have received a message that says that it has started.



- e. Minimize the **Command Prompt** window.  
Do not log off from the MUSE Application server, or the MUSE Holter formatting service will end.



If your system is using RDP, simply disconnect and allow the `museformat.exe` service to continue running.

**NOTE:**

If for any reason the `museformat.exe` process exits, it will need to be restarted by following step in the instructions above. It will be necessary to follow this process to manually restart the `museformat.exe` process whenever the MUSE application server is rebooted.

Issue	Probable Cause	Solution
Recently acquired MARS Holter reports are displaying squares instead of the correct Simplified Chinese characters in the MUSE v9 Editor.	The MUSE Format 2 service is still running as a windows service.	Follow the work instruction.. Each Holter test that shows this issue will have to be edited in some fashion and saved, which will cause the report to be re-formatted with the correct characters.
Recently acquired MARS Holter reports that are on the edit list cannot be opened repeatedly with the message that they are currently locked by the Administrator.	The <code>museformat.exe</code> is not running in a console window on the MUSE application server.	Follow the instructions in step 3. This will cause each report to be formatted and unlocked.





# Retrieving MUSE Error Logs on the SQL Server Management Studio

1. Open **SQL Server Management Studio**.
2. Select the **MUSE\_System** database.
3. Click **New Query**.  
A blank query window opens.
4. Type the following SQL query into the blank window, where <tablename> is replaced by the table name of the log that you want to retrieve.

```
SELECT * FROM <tablename>
```

The following table lists the <tablename> values for the associated logs.

MUSE Log	<tablename>
Application	logApplication
DICOM	logDicomTransaction
Acquisition	lognormal
Process	logProcess
HIS Event	logHISEvent
Print	logTransmit
Discard	logDiscard
Edit Change	logEditChange

5. Execute the query.  
Results are displayed.
6. Right-click in the results and select **Save Results As**.
7. Provide a file name and location and save the results.





## Holter Recreate Tool

This starts the process which will search all MUSE sites for Holter reports that were inserted into MUSE prior to MUSE v 9.0.0 that also have had a PDF created prior to MUSE v 9.0.4 (SP4). If for any reason the script is stopped it may be safely run multiple times. Once a Holter report has been regenerated the date of the PDF report will be updated in the database so it will not be selected by the script in subsequent runs. The script has a built-in throttle mechanism so that no more than 2 Holter reports are processed at one time as to not overload the format queue and/or lock out any reports coming in through the normal workflow process.

1. Log in to the MUSE application server as administrator.
2. Copy `MuseBackendTestingEngine.exe` and `HolterRecreate.xml` from the Support CD into the MUSE installation directory (default `C:\Program Files (x86)\Muse`).
3. Open a DOS window and navigate to the MUSE installation directory where you just copied the files.
4. Execute: `MuseBackendTestingEngine.exe -path:.-workflow:.\-HolterRecreate.xml`.





# Glossary

Term	Description
AD	<b>Active Directory.</b> Active Directory is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.
ADSI	<b>Active Directory Service Interfaces.</b> Active Directory Service Interfaces is a set of COM interfaces used to access the features of directory services from different network providers. ADSI is used in a distributed computing environment to present a single set of directory service interfaces for managing network resources.
archive	Permanent storage of data.
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.
backup	A spare copy of a file, file system or other resource for use in the event of failure or loss of the original.
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.
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.
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 that are transmitted via telephone to produce a paper copy of the graphics on the receiving fax machine.
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.
FTP	<b>File Transfer Protocol.</b> The method of moving files from system to system using TCP/IP.

Term	Description
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, this includes patient tracking, billing, and administrative programs. HIS can also include clinical features.
HL7	<b>Health Level 7.</b> A standard interface for exchanging and translating data between computer systems.
IEC	<b>International Electrotechnical Commission.</b> The international standards and conformity assessment body for all fields of electrotechnology.
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.
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.
LAN	<b>Local Area Network.</b> A data communications network that is geographically limited (typically to a 1 km radius) allowing easy interconnection of terminals, microprocessors, and computers within adjacent buildings.
LDAP	<b>Lightweight Directory Access Protocol.</b> LDAP is an application protocol used over an IP network to manage and access the distributed directory information service. Active Directory utilizes LDAP.
LED	<b>Light-Emitting Diode.</b> A type of diode that emits light when current passes through it.
NetBIOS	<b>Network Basic Input/Output System.</b> An applications programming interface (API) that activates network operations on IBM PC compatibles running under Microsoft's DOS. It is a set of network commands that the application program issues 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.
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 that makes equipment for example, computers) as opposed to one that 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.
PCL	<b>Printer Control Language.</b> A document description language used by Hewlett-Packard printers.



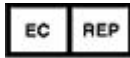
Term	Description
PDF	<b>Portable Document Format.</b> The native file format for Adobe Systems' Acrobat. PDF is the file format for representing documents in a manner that is independent of the original application software, hardware, and operating system used to create those documents.
PING	<b>Packet 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 is a programming language used by printers to describe the appearance of a printed page.
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.
ROM	<b>Read-Only Memory.</b> A type of data storage device that 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 and CD-ROM.
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.
UNC	<b>Universal Naming Convention.</b> The name given for the naming used when one specifies: \\the server\the volume\the path\then the file name of a file. An example of a UNC is: \\Myserver\Docdrive\Magazine\glossary.doc







GE Medical Systems  
*Information Technologies*, Inc.  
8200 West Tower Avenue  
Milwaukee, WI 53223 USA  
Tel: +1 414 355 5000  
+1 800 558 5120 (US Only)



GE Medical Systems  
*Information Technologies* GmbH  
Munzinger Straße 5  
79111 Freiburg Germany  
Tel: +49 761 45 43 -0

GE Medical Systems *Information Technologies*, Inc., a General Electric Company, going to market as GE Healthcare.

[www.gehealthcare.com](http://www.gehealthcare.com)

